2014

The Frobenius-Schur indicator of Tambara-Yamagami categories

Ryan T. Johnson
Iowa State University

The Frobenius-Schur indicator of Tambara-Yamagami categories

by

Ryan Timothy Johnson

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:

Tathagata Basak, Major Professor

Clifford Bergman

Leslie Hogben

Richard Ng

Amanda Weinstein

Iowa State University

Ames, Iowa

2014

DEDICATION

I would like to dedicate this thesis to my wife Heidi.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank everyone who has helped me write this thesis or in any other aspect of graduate school. In particular, I want to thank my advisor, Tathagata Basak, for all his help and guidance in the process of earning of my degree. I would also like to especially thank Richard Ng for suggesting the problem and for many encouraging and helpful discussions, as well as several excellent literature suggestions. I also want to thank the other members of my committee, Dr. Clifford Bergman, Dr. Leslie Hogben, and Dr. Amanda Weinstein, for their support. Special thanks goes to Melanie for all the assistance and advice that she has given me and all the other graduate students in the Mathematics department. Lastly, I want to thank my friends at Iowa State for all the fun these past five years.

ABSTRACT

In this thesis, we investigate the higher Frobenius-Schur indicator introduced by Ng and Schauenburg and prove that it is a strong enough invariant to distinguish between any two Tambara-Yamagami fusion categories. Our method of proof is based on computation of the Frobenius-Schur indicators as Gauss sums for certain quadratic forms on finite abelian groups and relies on the classification of quadratic forms on finite abelian groups due to Wall.

As a corollary to our work, we show that the state-sum invariants of 3-manifolds associated with Tambara-Yamagami categories determine the category as long as we restrict to Tambara-Yamagami categories defined coming from groups G whose order is not a power of 2. Turaev and Vainerman proved this result under the assumption that G has odd order and they conjectured that a similar result should hold for all Tambara-Yamagami categories. Their proof used the state-sum invariant of Lens spaces $L_{k,1}$. We provide an example showing that the state-sum invariants of Lens spaces is not enough to distinguish all Tambara-Yamagami categories.

CHAPTER 1. INTRODUCTION AND PRELIMINARIES

1.1 Introduction

Frobenius-Schur indicators were originally introduced in representation theory to determine whether a given irreducible representation of a compact group over a complex vector space admits a symmetric or a skew-symmetric invariant bilinear form. These indicators were later generalized to semisimple Hopf algebras by Linchenko and Montgomery [8] and to semisimple quasi-Hopf algebras by Mason and Ng [9]. Ng and Schauenburg developed the theory of Frobenius-Schur indicators in spherical fusion categories, see [13] and [14]. They defined the n-th Frobenius-Schur indicator $\nu_n(V)$ of an object V of such categories to be the trace of certain linear automorphism on $\mathrm{Hom}(\mathbf{1}, V^{\otimes n})$, where $\mathbf{1}$ is the neutral object.

A fusion category $\mathcal{C}$ is a $\mathbb{C}$-linear semisimple rigid monoidal (or tensor) category with finitely many simple objects and finite dimensional spaces of morphisms, such that the endomorphism algebra of the neutral object is $\mathbb{C}$ (see [1]). According to Etingof, Nikshych, and Ostrik in [3], fusion categories arise in several areas of mathematics and physics – conformal field theory, operator algebras, representation theory of quantum groups, and others.

Let G be a finite abelian group. Tambara and Yamagami [19] proved that equivalence classes of fusion categories with simple objects $S := G \cup \{m\}$ and fusion rules $a \otimes b \cong a + b$, $a \otimes m \cong m \cong m \otimes a$ with $a, b \in G$ and $m \otimes m \cong \bigoplus_{x \in G} x$ are parametrized by pairs (χ, τ) where χ is a non-degenerate symmetric bicharacter on G and $\tau = \pm |G|^{-1/2}$. Shimizu in [17] considered these categories and found a closed formula for the indicator. The main result of this thesis is proving that the Frobenius-Scour indicator is a strong enough invariant that inequivalent Tamabara-Yamagami categories will have differing Frobenius-Schur indicators for some integer k.

According to Turaev and Vainerman in [20], "one of the fundamental achievements of quantum topology was a discovery of a non-trivial connection between monoidal categories and 3-manifolds. This connection was first observed by O. Viro and V. Turaev and later generalized in the papers of J. Barrett, B. Westbury, A. Ocneanu, S. Gelfand, D. Kazhdan, and others. Their results may be summarized by saying that every spherical fusion category $\mathcal{C}$ over $\mathbb{C}$ with $\mathrm{pdim}(\mathcal{C}) \neq 0$ gives rise to a topological invariant $|M|_{\mathcal{C}} \in \mathbb{C}$ of any closed manifold M." Turaev and Vainerman proved that these invariants are enough to distinguish Tambara-Yamagami categories when the underlying groups are of odd order. The method was using the Reshetikhin-Turaev invariant on lens spaces $L_{k,1}$ for positive k. They also conjectured that the state-sums of 3-manifolds are enough to distinguish all Tambara-Yamagami categories. At the end of this thesis we are able to make a stronger positive statement than that found in [20] and also exhibit two Tambara-Yamagami categories $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $|L_{k,1}|_{\mathcal{C}_1} = |L_{k,1}|_{\mathcal{C}_2}$ for all non-negative k. This shows that the state-sums of the lens spaces are not enough to prove the conjecture true.

1.2 Overview of Thesis

In the remainder of this chapter, we cover the necessary category theory. In section 3 we give fundamental definitions and facts of spherical fusion categories. Much of the material in that section can be found in [1], [3], and [6]. In section 4 we define the Frobenius-Schur indicator and present a major theorem from Ng and Schauenburg in [13] that uses the center construction to express the Frobenius-Schur indicator in another form.

Chapter 2 is devoted to bilinear and quadratic forms. Section 1 covers basic facts and definitions, as well as a statement about the relations between quadratic and bilinear forms. Section 2 proves that every bilinear or quadratic form is an orthogonal direct sum of irreducibles. The results here are mostly due to Wall in [21]. See also [11], [7], and [15]. In Section 3 we define a new tensor notation for bilinear and quadratic forms. Section 4 provides many Gauss sums that will be required in the following chapter.

Chapter 3 contains the main results of this thesis. We define Tambara-Yamagami categories in Section 1. In Section 2 we exhibit proofs for two results from Shimizu [17]. The second is

proved in a different way using Milgram's formula. Section 3 contains our main result. We use our tensor notation to express the Frobenius-Schur indicator in terms of Gauss sums of the original group. Then using the diagonalization from chapter 2 section 2 and the Gauss sums computed in chapter 2 section 4 we prove that the Frobenius-Schur indicator is a strong enough invariant to distinguish between different Tambara-Yamagami categories. In section 4 we reference the state-sum invariant as defined in [20] and give an example that shows that the state-sum invariant of the Lens spaces $L_{k,1}$ is not a strong enough invariant to distinguish between all Tambara-Yamagami categories.

1.3 Spherical Fusion Categories

Our computations of Frobenius-Schur indicators will be based on the theorem at the end of this chapter. The following two sections introduce the necessary definitions and facts for giving the background of that theorem.

We will work over the field of complex numbers $\mathbb{C}$. We denote by μ_n the n-th roots of unity in $\mathbb{C}$, and μ_∞ will denote all roots of unity. We will give certain facts and definitions of spherical fusion categories. The reader may refer to [1], see [3], and [6] for more information.

Definition 1.3.1. A $\mathbb{C}$-*linear category* $\mathcal{C}$ is a category enriched over, $\mathrm{Vect}_{\mathbb{C}}$, the category of complex vector spaces. Equivalently, the Hom-spaces of $\mathcal{C}$ are $\mathbb{C}$-vector spaces and composition of morphisms is associative and bilinear.

Definition 1.3.2. An object U of a $\mathbb{C}$-linear category is called *simple* if any injection $V \hookrightarrow U$ is either 0 or an isomorphism.

A $\mathbb{C}$-*linear semisimple category* $\mathcal{C}$ is a $\mathbb{C}$-linear category such that all objects are finite direct sums of simple ones.

Remark 1.3.3. By Schur's Lemma, U is a simple object of $\mathcal{C}$ if and only if $\mathrm{End}(U) \cong \mathbb{C}$.

Definition 1.3.4. A *monoidal* (or *tensor*) category is a category $\mathcal{C}$ equipeed with

- a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ called the *tensor product*,
- an object $\mathbf{1}$ called the *unit object* or *identity object*,

- three natural isomorphisms subject to certain coherence conditions expressing the fact that the tensor product
  - is associative: there is a natural isomorphism Φ called *associator*, with components
$$\Phi_{V,W,U} : (V \otimes W) \otimes U \to V \otimes (W \otimes U)$$
  - has $\mathbf{1}$ as left and right identity: there are two natural isomorphisms l and r, respectively called *left* and *right unitor* with components
$$l_V : \mathbf{1} \otimes V \to V \quad \text{and} \quad r_V : V \otimes \mathbf{1} \to V$$

The coherence conditions for these natural transformations are:

- For all objects V_1, V_2, V_3, and V_4 in $\mathcal{C}$, the pentagon diagram in Figure 1.1 commutes.

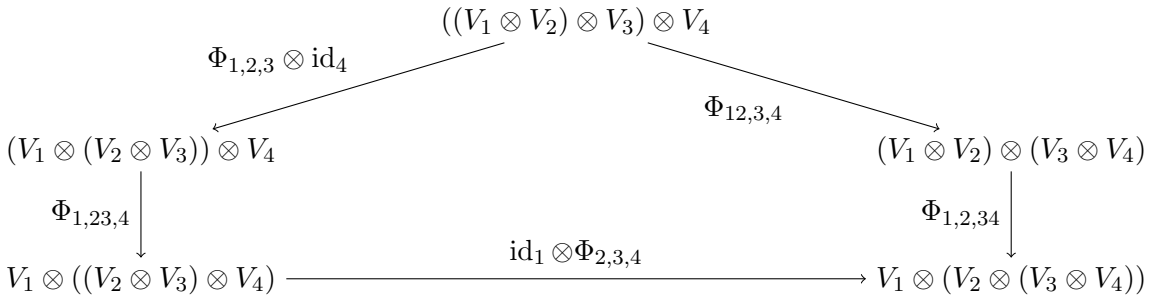

Figure 1.1 Pentagon Axiom

- For all objects V_1 and V_2 in $\mathcal{C}$ the triangle diagram in Figure 1.2 commutes.

By the following theorem, we may assume that the unit object in a monoidal category is *strict*, that is, that for any object V in $\mathcal{C}$ we have $\mathbf{1} \otimes V = V = V \otimes \mathbf{1}$.

Theorem 1.3.5 ([16], Theorem 3.2)**.** *Let $(\mathcal{C}, \otimes, \mathbf{1}, \Phi, l, r)$ be a monoidal category, and let $\mathbf{1}'$ be any object of $\mathcal{C}$ isomorphic to $\mathbf{1}$. Then there is an equivalent monoidal category $(\mathcal{C}, \otimes', \mathbf{1}', \Phi', l', r')$ in which l' and r' are identities.*

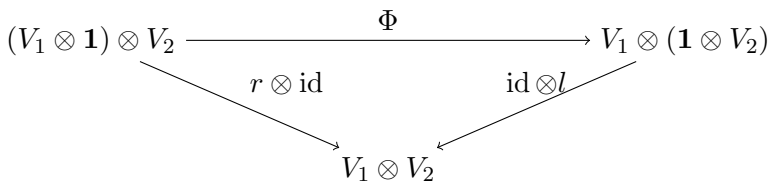

Figure 1.2 Triangle Axiom

We will also use Mac Lane's Coherence Theorem in the next section.

Theorem 1.3.6 (Mac Lane Coherence Theorem)**.** *Any monoidal category* $(\mathcal{C}, \otimes, \mathbf{1}, \Phi, l, r)$ *is monoidally equivalent to a strict monoidal category* $(\mathcal{C}', \otimes', \mathbf{1}', \mathrm{id}, \mathrm{id}, \mathrm{id})$.

Definition 1.3.7. Let $\mathcal{C}$ be a monoidal category. Let X and Y be objects of $\mathcal{C}$ formed by tensoring the same sequence of objects V_1,...,V_n in $\mathcal{C}$, only with different placement of parentheses, then there is a unique morphism $\Phi^? : X \to Y$ composed formally from instances of Φ and Φ^{-1}. Note that we are using the same notation as that used in [14].

Definition 1.3.8. Let $\mathcal{C}$ be a monoidal category. Let V be an object of $\mathcal{C}$. A *left dual* of V is a triple $(V^*, \mathrm{ev}, \mathrm{coev})$ where

- V^* is an object of the category,
- ev and coev are natural transformations with components $\mathrm{ev}_V : V^* \otimes V \to \mathbf{1}$ and $\mathrm{coev}_V : \mathbf{1} \to V \otimes V^*$ such that the diagrams in Figure 1.3 commute.

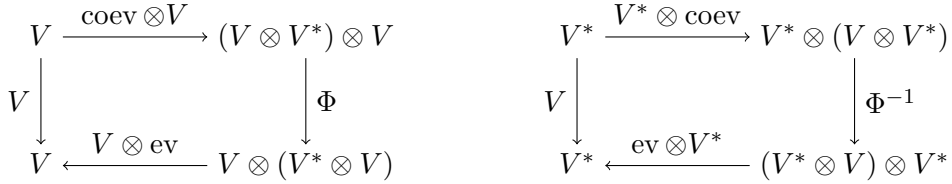

Figure 1.3 Duality Diagrams

A *right dual* of V is a left dual of V in $\mathcal{C}^{\mathrm{sym}}$, the category $\mathcal{C}$ with the tensor defined in the reverse order.

Lemma 1.3.9 ([6]). *Let $\mathcal{C}$ be a monoidal category and let V be an object of $\mathcal{C}$ such that V has a two left duals $(V^*, \mathrm{ev}, \mathrm{coev})$ and $(V^\star, \mathrm{ev}', \mathrm{coev})$. Then there exists a unique isomorphism $f : V^\star \to V^*$ such that $\mathrm{ev}'_V = \mathrm{ev}_V \circ (V \otimes f)$ and $\mathrm{coev}_V = (V \otimes f) \circ \mathrm{coev}'_V$.*

The same is true for right duals.

Definition 1.3.10. A *left (right) rigid monoidal category* is a monoidal category $\mathcal{C}$ such that every object V in $\mathcal{C}$ has a left (right) dual. A category that is both left rigid and right rigid is simply called a *rigid monoidal category.*

Remark 1.3.11. Let V and W be objects of $\mathcal{C}$. One may check that $(W^* \otimes V^*, \mathrm{ev}_{V\otimes W}, \mathrm{coev}_{V\otimes W})$ is a left dual of $V \otimes W$ where $\mathrm{ev}_{V\otimes W}$ and $\mathrm{coev}_{V\otimes W}$ are appropriate compositions of ev, coev, and Φ.

Definition 1.3.12. Let $\mathcal{C}$ be a left-rigid monoidal category. A *pivotal structure* j is a monoidal natural isomorphism with components $j_V : V \to V^{**}$. A *pivotal monoidal category* is a left-rigid monoidal category with a pivotal structure.

Lemma 1.3.13. *Let $\mathcal{C}$ be a left-rigid monoidal category with a pivotal structure. Then $\mathcal{C}$ is rigid.*

Proof. Let V be an object of $\mathcal{C}$. Then one may check that

$$(V^*, \mathrm{ev}_{V^*} \circ (j_V \otimes V^*), (V^* \otimes j_V^{-1}) \circ \mathrm{coev}_{V^*})$$

is a right dual of V. □

Definition 1.3.14. Let $\mathcal{C}$ be a pivotal monoidal category with pivotal structure j.

1. For an endomorphism $f : V \to V$ we define the left and right *pivotal trace* to be

$$\mathrm{ptr}^r(f) = \mathrm{ev}_{V^*} \circ (j_V \otimes V^*) \circ (f \otimes V^*) \circ \mathrm{coev}_{V^*}$$
$$\mathrm{prt}^l(f) = \mathrm{ev}_V \circ (V^* \otimes f) \circ (V^* \otimes j_V^{-1}) \circ \mathrm{coev}_V$$

2. If $\mathrm{ptr}^r(f) = \mathrm{ptr}^l(f)$ for all endomorphisms f in $\mathcal{C}$ then $\mathcal{C}$ is called *spherical* and we simply use the notation $\mathrm{ptr}(f)$.

3. If V is an object of a spherical monoidal category we define the *pivotal dimension* of V as $\mathrm{pdim}(V) = \mathrm{ptr}(\mathrm{id}_V)$.

4. If $\mathcal{C}$ is a $\mathbb{C}$-linear semisimple spherical category we define the *pivotal dimension* of $\mathcal{C}$ to be
$$\mathrm{pdim}(\mathcal{C}) = \sum_{V \in \Gamma} |\,\mathrm{pdim}(V)|^2$$
where Γ is the set of isomorphism classes of simple objects.

Definition 1.3.15. A *fusion category* $\mathcal{C}$ over $\mathbb{C}$ is a $\mathbb{C}$-linear semisimple rigid monoidal category with finitely many isomorphism classes of simple objects and finite dimensional Hom-spaces, such that the unital object is a simple object.

A *pivotal (spherical) fusion category* is a fusion category with a pivotal (spherical) structure.

A *strict pivotal (spherical) monoidal category* is a pivotal (spherical) monoidal category such that Φ, l, r, j are all identity morphisms and for all objects V and W of the category $(V \otimes W)^* = W^* \otimes V^*$.

Theorem 1.3.16 ([14], Theorem 2.2)**.** *Any pivotal monoidal category is equivalent, as a pivotal monoidal category, to a strict pivotal monoidal category.*

Remark 1.3.17. Let $\mathcal{C}$ be a monoidal category. Let X and Y be objects of $\mathcal{C}$ formed by tensoring the same sequence of objects V_1,...,V_n in $\mathcal{C}$, only with different placement of parentheses, then there is a unique morphism $\Phi^? : X \to Y$ composed formally from instances of Φ and Φ^{-1}. Note that we are using the same notation as that used in [14].

1.4 The Frobenius Schur Indicator

Definition 1.4.1. Let $\mathcal{C}$ be a monoidal category. A *braiding* is a natural isomorphism with components $c_{V,W} : V \otimes W \to W \otimes V$ which satisfies the two braid relations

$$\Phi \circ c_{V,Y\otimes Z} \circ \Phi = (\mathrm{id}_Y \otimes c_{V,Z}) \circ \Phi \circ (c_{V,Y} \otimes \mathrm{id}_Z) \quad \text{for all } V, Y, Z \in \mathcal{C}$$
$$\Phi^{-1} \circ c_{Y\otimes Z,V} \circ \Phi^{-1} = (c_{Y,V} \otimes \mathrm{id}_Z) \circ \Phi^{-1} \circ (\mathrm{id}_Y \otimes c_{Z,V}) \quad \text{for all } V, Y, Z \in \mathcal{C}$$

A *braided monoidal category* is a monoidal category with a braiding.

Definition 1.4.2. A *ribbon category* is a braided spherical fusion category. Note: this is a stronger definition than others found in the literature. For instance, [1] does not require ribbon categories to be semisimple.

Let $\mathcal{C}$ be a ribbon category. The *twist* θ is a natural isomorphism with components

$$\theta_V = (\mathrm{ev}_V \otimes j_V^{-1}) \circ \Phi^{-1} \circ (\mathrm{id}_{V^*} \otimes c_{V^{**},V}) \circ \Phi \circ (\mathrm{coev}_{V^*} \otimes \mathrm{id}_V)$$

Definition 1.4.3. Let $\mathcal{C}$ be a monoidal category and let $V \in \mathcal{C}$. A *half braiding* e_V for V is a family $\{e_V(W) \in \mathrm{Hom}(V \otimes W, W \otimes V), W \in \mathcal{C}\}$ of morphisms satisfying

1. Naturality with regard to the argument in parentheses

$$(f \otimes \mathrm{id}_V) \circ e_V(Y) = e_V(Z) \circ (\mathrm{id}_V \otimes f) \text{ for all } f \in \mathrm{Hom}(Y, Z).$$

2. The braid relation

$$\Phi \circ e_V(Y \otimes Z) \circ \Phi = (\mathrm{id}_Y \otimes e_V(Z)) \circ \Phi \circ (e_V(Y) \otimes \mathrm{id}_Z) \text{ for all } Y, Z \in \mathcal{C}.$$

3. All $e_V(X)$ are isomorphisms.

4. The unit property

$$e_V(\mathbf{1}) = \mathrm{id}_V$$

Definition 1.4.4. The (left) center $\mathcal{Z}(\mathcal{C})$ of a monoidal category C has as objects pairs (V, e_V) where $V \in \mathcal{C}$ and e_V is a half braiding. A morphisms $f \in \mathrm{Hom}_{\mathcal{Z}(\mathcal{C})}((V, e_V), (W, e_W))$ is a morphism $f \in \mathrm{Hom}_{\mathcal{C}}(V, W)$ such that

$$(\mathrm{id}_V \otimes f) \circ e_V(Z) = e_W(Z) \circ (f \otimes \mathrm{id}_V) \text{ for all } Z \in \mathcal{C}$$

The tensor product of objects is given by $(V, e_V) \otimes (W, e_W) = (V \otimes W, e_{V \otimes W})$, where

$$e_{V \otimes W}(Z) = \Phi \circ (e_V(Z) \otimes \mathrm{id}_W) \circ \Phi^{-1} \circ (\mathrm{id}_V \otimes e_W(Z)) \circ \Phi \text{ for all } Z \in \mathcal{C}$$

The tensor unit is $(\mathbf{1}, e_{\mathbf{1}})$ where $e_{\mathbf{1}}(V) = \mathrm{id}_V$ for all $V \in \mathcal{C}$. The composition and tensor product of morphisms are inherited from $\mathcal{C}$. The braiding is given by

$$c((V, e_V), (W, e_W)) = e_V(W) \text{ for all } V, W \in \mathcal{C}$$

Remark 1.4.5. It is important to note the abuse of notation in the two definitions above. Given $V \in \mathcal{C}$, it is possible (and likely) that there are more than one half braidings e_V corresponding to V.

Theorem 1.4.6 ([12], Section 3)**.** *Let $\mathcal{C}$ be a spherical fusion category. Then $\mathcal{Z}(\mathcal{C})$ is a ribbon category.*

Lemma 1.4.7 ([12], Section 8)**.** *Let $\mathcal{C}$ be a spherical fusion category and let $\mathcal{Z}(\mathcal{C})$ be the (left) center of $\mathcal{C}$. Then the forgetful functor mapping $(V, e_V) \mapsto V$ has a two-sided adjoint*

$$K_{\mathcal{C}}(V) = \bigoplus_{(X,e_X)\in\hat{\Gamma}} (X, e_X) \dim\left(\mathrm{Hom}_{\mathcal{C}}(X, V)\right)$$

where $\hat{\Gamma}$ is the set of isomorphism classes of simple objects in $\mathcal{Z}(\mathcal{C})$.

Next we would like to define the indicator.

Definition 1.4.8. Let $\mathcal{C}$ be a rigid monoidal category and let V and W be objects of $\mathcal{C}$. It is well known that

- $A_{V,W} : \mathrm{Hom}(\mathbf{1}, V \otimes W) \to \mathrm{Hom}(V^*, W)$ defined by

$$A_{V,W}(f) = (\mathrm{ev}_V \otimes W) \circ \Phi^{-1}_{V^*,V,W} \circ (V^* \otimes f)$$

- $B_{V,W} : \mathrm{Hom}(V, W) \to \mathrm{Hom}(\mathbf{1}, W \otimes V^*)$ defined by

$$B_{V,W}(g) = (g \otimes V^*) \circ \mathrm{coev}_{V^*}$$

are natural isomorphisms in $V, W \in \mathcal{C}$ [6], XIV.2.2.

Definition 1.4.9. Let $\mathcal{C}$ be a monoidal category and $V \in \mathcal{C}$. Let $V^{\otimes n}$ be defined inductively by $V^{\otimes 0} = \mathbf{1}$, $V^{\otimes 1} = V$ and $V^{\otimes n} = V \otimes V^{\otimes(n-1)}$.

Let $\Phi^{(n)}$ be the unique isomorphism $\Phi^? : V^{\otimes(n-1)} \otimes V \to V^{\otimes n}$.

Definition 1.4.10. Let $\mathcal{C}$ be pivotal monoidal category and $V \in \mathcal{C}$. Let $E_V^{(n)} : \mathrm{Hom}(\mathbf{1}, V^{\otimes n}) \to \mathrm{Hom}(\mathbf{1}, V^{\otimes n})$ be defined by

$$E_V^{(n)}(f) = \Phi^{(n)} \circ (\mathrm{id}_{V^{\otimes(n-1)}} \otimes j_V^{-1}) \circ \left(B_{V^*,V^{\otimes(n-1)}} A_{V,V^{\otimes n}}\right)(f)$$

The *n-th Frobenius-Schur indicator* $\nu_n(V)$ is defined by

$$\nu_n(V) = \mathrm{Tr}\left(E_V^{(n)}\right)$$

where Tr is the usual trace of linear maps.

Theorem 1.4.11 ([13], Theorem 4.1)**.** *Let $\mathcal{C}$ be a spherical fusion category and let $V \in \mathcal{C}$. Then*

$$\begin{aligned}\nu_n(V) &= \frac{1}{\mathrm{pdim}(\mathcal{C})}\,\mathrm{ptr}\left(\theta_{K(V)}^n\right)\\ &= \frac{1}{\mathrm{pdim}(\mathcal{C})}\sum_{(X,e_X)\in\hat{\Gamma}}\theta_{(X,e_X)}^n\,\mathrm{pdim}(X)\,\dim(\mathrm{Hom}(V,X))\end{aligned}$$

where $\hat{\Gamma}$ is the set of isomorphism classes of simple obejcts of $\mathcal{Z}(\mathcal{C})$, K is the functor from Lemma 1.4.7, and θ is the twist of $\mathcal{Z}(\mathcal{C})$.

CHAPTER 2. BILINEAR AND QUADRATIC FORMS ON FINITE ABELIAN GROUPS

2.1 Terms and p-valuation

Definition 2.1.1. 1. Let p be a prime. Define the abelian group $\mathbb{Q}_{(p)} = \left\{ \frac{m}{p^r} : m, r \in \mathbb{Z} \right\}$.

2. For G a finite abelian group and k a positive integer. Let $G[k] = \{g \in G : kg = 0\}$.

3. Define $\overline{\mathbb{Z}} = \mathbb{Z} \cup \{\infty\}$ to be the semi group such that $n + \infty = \infty = \infty + \infty$, and let $\overline{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ be defined similarly.

4. Let $\mathbf{e} : \overline{\mathbb{Q}} \to \mu_\infty \cup \{0\}$ be defined by

$$\mathbf{e}(x) = \begin{cases} e^{2\pi i x} & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x = \infty \end{cases}$$

Definition 2.1.2 (p-valuation)**.** Let p be a rational prime. Let G be a group such that the order of every element is a power of p. Let g be a non-zero element of G. Let $v_p : G \to \overline{\mathbb{Z}}$ be defined by $v_p(g) = -\log_p |g|$. So $-v_p(g)$ is the least non-negative integer such that $p^{-v_p(g)} g = 0$. One has

$$|g| = p^{-v_p(g)}$$

We also let $v_p(0) = \infty$. We say that $v_p(g)$ is the *p-valuation* of g.

We will also use the traditional p-valuation on integers. Let $v_p(n)$ be the integer such that $n = p^{v_p(n)} n'$ where n' is relatively prime to p. Again we let $v_p(0) = \infty$.

Lemma 2.1.3. *Let p be a prime and G be a p-group.*

(a) Let $g \in G$ and $n \in \mathbb{Z}$. Then $ng = 0$ if and only if $v_p(n) + v_p(g) \geq 0$. In particular, $p^r g = 0$ if and only if $v_p(g) \geq -r$.

(b) Let $g \in G$ and $n \in \mathbb{Z}$ such that $ng \neq 0$, then $v_p(n) + v_p(g) = v_p(ng)$.

(c) Let $g, h \in G$. Then $v_p(g+h) \geq \min\{v_p(g), v_p(h)\}$.

(d) For $g, h \in G$ $v_p(g+h) = \min\{v_p(g), v_p(h)\}$ if $v_p(g) \neq v_p(h)$ or if $\langle g \rangle \cap \langle h \rangle = 0$.

Proof. (a) The statement is true if either n or g is zero. If both n and g are nonzero then $n = p^{v_p(n)}n'$ for some n' relatively prime to p and $|g| = p^{-v_p(g)}$. The fact that $ng = 0$ can thus be expressed as $v_p(n) \geq -v_p(g)$. This proves the statement.

(b) Again write $n = p^{v_p(n)}n'$ for some n' relatively prime to p. Since $ng \neq 0$ we have $p^{v_p(n)}g \neq 0$. So $v_p(n) < -v_p(g)$. We have $p^{-v_p(g)-v_p(n)}ng = n'p^{-v_p(g)}g = 0$. So $v_p(ng) \geq v_p(n) + v_p(g)$. On the other hand

$$0 = p^{-v_p(ng)}ng = n'p^{v_p(n)-v_p(ng)}g$$

So $v_p(n) - v_p(ng) \geq -v_p(g)$. This proves the statement.

(c) Let $g, h \in G$. Let $r = \min\{v_p(g), v_p(h)\}$. Then $p^{-r}g = 0$ and $p^{-r}h = 0$ and thus $p^{-r}(g+h) = 0$. So $v_p(g+h) \geq r$, which completes the proof.

(d) Let $g, h \in G$ such that $v_p(g) \neq v_p(h)$. Without loss of generality let $v_p(g) < v_p(h)$. Then

$$p^{-v_p(g)-1}(g+h) = p^{-v_p(h)-1}g + 0 \neq 0$$

Then part (c) implies $v_p(g+h) = v_p(g)$.

Let $g, h \in G$ such that $\langle g \rangle \cap \langle h \rangle = 0$. Let $r = \min\{v_p(g), v_p(h)\}$. Then $p^{r-1}g \neq 0$ or $p^{r-1}h \neq 0$ or both. By our assumption, in all cases $p^{r-1}(g+h) \neq 0$. Part (c) implies $v_p(g+h) = r$. □

Definition 2.1.4. Let G be a finite abelian group (written additively). A *symmetric bilinear form* on G is a function $b : G \times G \to \mathbb{Q}/\mathbb{Z}$ such that for all $x, y, z \in G$,

$$b(x, y) = b(y, x)$$

$$b(x + y, z) = b(x, z) + b(y, z).$$

It follows that for each $x \in G$, the functions $b(x, \cdot) : G \to \mathbb{Q}/\mathbb{Z}$ and $b(\cdot, x) : G \to \mathbb{Q}/\mathbb{Z}$ are $\mathbb{Z}$-module homomorphisms. Note that a bilinear form b on G takes values in $\exp(G)^{-1}\mathbb{Z}/\mathbb{Z}$.

Define the *radical* of b to be the subgroup $\mathrm{Rad}(b) = \{x \in G : b(x,y) = 0 \text{ for all } y \in G\}$. A *discriminant form* is a pair (G,b) where G is a finite abelian group and b is a symmetric bilinear form on G. A *morphism of discriminant forms* $f : (G_1,b_1) \to (G_2,b_2)$ is a group homomorphism $f : G_1 \to G_2$ such that $b_1 = b_2 \circ (f \times f)$. Say that b or (G,b) is *non-degenerate* if $\mathrm{Rad}(b) = 0$.

Definition 2.1.5. Given a function $q : G \to \mathbb{Q}/\mathbb{Z}$, we define $b_q : G \times G \to \mathbb{Q}/\mathbb{Z}$ by

$$b_q(x,y) = q(x+y) - q(x) - q(y).$$

Lemma 2.1.6. *Let $q : G \to \mathbb{Q}/\mathbb{Z}$ be any function. Let $x,y,z \in G$. TFAE:*

1. $q(x+y+z) + q(x) + q(y) + q(z) = q(x+y) + q(x+z) + q(y+z)$.
2. $b_q(x+y,z) = b_q(x,z) + b_q(y,z)$.
3. $b_q(x,y+z) = b_q(x,y) + b_q(x,z)$.

Proof. Write 2 and 3 in terms of q and they become 1. □

Lemma 2.1.7. *Let $q : G \to \mathbb{Q}/\mathbb{Z}$ be a function. The following are equivalent:*

1. *For all $x,y,z \in G$ $q(-x) = q(x)$ and*
$$q(x+y+z) + q(x) + q(y) + q(z) = q(x+y) + q(x+z) + q(y+z)$$
2. *The function $b_q : G \times G \to \mathbb{Q}/\mathbb{Z}$ is bilinear and $q(-x) = q(x)$ for all $x \in G$.*
3. *The function $b_q : G \times G \to \mathbb{Q}/\mathbb{Z}$ is bilinear and $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}$, $x \in G$.*

Proof. The equivalence of 1 and 2 follows from Lemma 2.1.6. Clearly 3 implies 2. It remains to prove 2 implies 3. Assume 2. Note that

$$q(0) = q(0) + q(0) - q(0+0) = -b_q(0,0) = 0.$$

One has

$$b_q(x,x) = -b_q(x,-x) = q(x) + q(-x) - q(x-x) = 2q(x)$$

for all $x \in G$. Suppose $q(mx) = m^2 q(x)$ for some $m \geq 1$. Then

$$q((m+1)x) = q(mx) + q(x) + b_q(mx, x) = m^2 q(x) + q(x) + 2mb_q(x, x) = (m+1)^2 q(x).$$

By induction on m it follows that $q(mx) = m^2 q(x)$ for all $m \in \mathbb{N}$. If m is a negative integer, then $q(mx) = q(-mx) = (-m)^2 q(x) = m^2 q(x)$. □

Definition 2.1.8. Say that $q : G \to \mathbb{Q}/\mathbb{Z}$ is a *quadratic form* on G if q satisfies the equivalent conditions in Lemma 2.1.7. In this case b_q is called the *bilinear form associated to the quadratic form* q. A *pre-metric group* is a pair (G, q) where G is a finite abelian group and q is a quadratic form on G. A pre-metric group (G, q) is called a *metric group* if b_q is non-degenerate.

For any quadratic form or pre-metric group define $\mathrm{Rad}(q) = \mathrm{Rad}(G, q) = \mathrm{Rad}(b_q)$. Say that q or (G, q) is non-degenerate if $\mathrm{Rad}(q) = 0$.

Lemma 2.1.9. *(a) Let (G, q) be a pre-metric p-group. Let $p^r = \exp(G)$ for some r. Then b_q takes values in $p^{-r}\mathbb{Z}/\mathbb{Z}$. If p is odd, q takes values in $p^{-r}\mathbb{Z}/\mathbb{Z}$. If $p = 2$, q takes values in $2^{-r-1}\mathbb{Z}/\mathbb{Z}$. (b) Let (G, q) be a pre-metric group. Then for $g_1, ..., g_n \in G$,*

$$q\left(\sum_{i=1}^{n} g_i\right) = \sum_{i=1}^{n} q(g_i) + \sum_{1 \leq i < j \leq n} b_q(g_i, g_j).$$

Proof. (a) For any $g, h \in G$, $p^r b_q(g, h) = b_q(p^r g, h) = 0$. The other two statements follow from the fact that $2q(g) = b_q(g, g)$ for all $g \in G$.

The proof of (b) is inductive from $q(g_1 + g_2) = q(g_1) + q(g_2) + b_q(g_1, g_2)$. □

Definition 2.1.10. Let **Bil** be the category of discriminant forms. Let $(G, b), (H_1, b_1), (H_2, b_2) \in$ **Bil** such that $G = H_1 \oplus H_2$ and for all $h_1, h_1' \in H_1$ and $h_2, h_2' \in H_2$

$$b(h_1 + h_2, h_1' + h_2') = b_1(h_1, h_1') + b_2(h_2, h_2').$$

Then we say (G, b) is an *orthogonal direct sum* of (H_1, b_1) and (H_2, b_2). We will use the notation

$$(G, b) = (H_1, b_1) \perp (H_2, b_2).$$

A discriminant form is *irreducible* if it is not an orthogonal direct sum of two non-zero discriminant forms. Let **Quad** be the category of pre-metric groups. For $(G, q), (H, \mu) \in$ **Quad** let the orthogonal direct sum be defined by

$$(G_1, q_1) \perp (G_2, q_2) = (G_1 \oplus G_2, q) \quad \text{where} \quad q(g_1 + g_2) = q_1(g_1) + q_2(g_2) \quad \text{for} \quad g_1 \in G_1, g_2 \in G_2$$

Remark 2.1.11. Let $F : \mathbf{Quad} \to \mathbf{Bil}$ be the functor defined by the mapping $(G, q) \mapsto (G, b_q)$. Then F preserves orthogonal direct sums.

Proof. Let $(G_1, q_1), (G_2, q_2) \in \mathbf{Quad}$. Let $(G, q) = (G_1, q_1) \perp (G_2, q_2)$. Then for $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$

$$\begin{aligned} b_q(g_1 + g_2, h_1 + h_2) &= q(g_1 + g_2 + h_1 + h_2) - q(g_1 + g_2) - q(h_1 + h_2) \\ &= q_1(g_1 + h_1) + q_2(g_2 + h_2) - q_1(g_1) - q_2(g_2) - q_1(h_1) - q_2(h_2) \\ &= b_{q_1}(g_1, h_1) + b_{q_2}(g_2, h_2) \end{aligned}$$

Thus $(G, b_q) = (G_1, b_{q_1}) \perp (G_2, b_{q_2})$. □

Definition 2.1.12. Let (G, b) be a discriminant form. Let $e_1, \cdots, e_k \in G$ and $b_{ij} = b(e_i, e_j)$. The matrix $\text{gram}_b(e_1, ...e_n) = B = (\!(b_{ij})\!)$ is called the *gram matrix* of $e_1, \cdots, e_k$. One has

$$b(\sum_i g_i e_i, \sum_i h_j e_j) = (g_1, \cdots, g_k)B(h_1, \cdots, h_k)^{tr} \text{ for all } g_j, h_j \in \mathbb{Z}.$$

A finite abelian group is *homogeneous* if it is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^n$ for some prime p and positive integers r and n. An element of $(\mathbb{Z}/p^r\mathbb{Z})^n$ will often be written as a vector whose entries come from $\mathbb{Z}/p^r\mathbb{Z}$. A discriminant form on a homogeneous finite abelian group will be often written down as $((\mathbb{Z}/p^r\mathbb{Z})^n, B)$ where B is a $n \times n$ matrix with entries in $p^{-r}\mathbb{Z}/\mathbb{Z}$ such that $b(x, y) = x^{tr}By$ for all $x, y \in (\mathbb{Z}/p^r\mathbb{Z})^n$. Let p be an odd prime and u_p denote a quadratic non-residue modulo p. Table 2.1 lists the irreducible metric groups (G, q) and corresponding irreducible discriminant forms (G, b_q). This will be proven in the next section.

2.2 The Block Diagonalization of Bilinear and Quadratic Forms

The following section leads up to the final theorem which states that Table 2.1 contains all irreducible discriminant forms and metric groups. The case of discriminant forms is proven in [21] section 5. In that paper, Wall constructs a bijection between discriminant forms and (possibly smaller) metric groups. We are not concerned with this bijection, but simply the block-diagonalization of metric groups and the fact that for each discriminant form (G, b) there exists at least one metric group (G, q) such that $b_q = b$.

name (from [11])	(G,q)	(G,b_q)
A_{p^r}	$\left(\mathbb{Z}/p^r\mathbb{Z}, q(x)=\frac{(p^r+1)/2}{p^r}x^2\right)$	$\left(\mathbb{Z}/p^r\mathbb{Z}, \frac{1}{p^r}\right)$
B_{p^r}	$\left(\mathbb{Z}/p^r\mathbb{Z}, q(x)=\frac{u_p(p^r+1)/2}{p^r}x^2\right)$	$\left(\mathbb{Z}/p^r\mathbb{Z}, \frac{u_p}{p^r}\right)$
A_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x)=\frac{1}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{1}{2^r}\right)$
B_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x)=\frac{-1}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{-1}{2^r}\right)$
C_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x)=\frac{5}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{5}{2^r}\right)$
D_{2^r}	$\left(\mathbb{Z}/2^r\mathbb{Z}, q(x)=\frac{-5}{2^{r+1}}x^2\right)$	$\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{-5}{2^r}\right)$
E_{2^r}	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, q(x_1,x_2)=\frac{x_1x_2}{2^r}\right)$	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, \left(\begin{smallmatrix}0 & 2^{-r}\\ 2^{-r} & 0\end{smallmatrix}\right)\right)$
F_{2^r}	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, q(x_1,x_2)=\frac{x_1^2+x_1x_2+x_2^2}{2^r}\right)$	$\left((\mathbb{Z}/2^r\mathbb{Z})^2, \left(\begin{smallmatrix}2^{1-r} & 2^{-r}\\ 2^{-r} & 2^{1-r}\end{smallmatrix}\right)\right)$

Table 2.1 Irreducible quadratic and bilinear forms

If one looks closely at the table above, one may see that all of the "trouble" with finding a bijection between discriminant forms and metric groups of the same size lies in the case when $p = 2$ and $r < 3$ in which some of the types are not distinct. Even worse, some of the metric group types are distinct, but their matching discriminant forms are not. Thus, if $|G|$ is even it is possible for a discriminant form (G, b) to have several metric groups (G, q_i) such that $b_{q_i} = b$.

Lemma 2.2.1. *Let (G,b) be a discriminant form. Let $\{p_1, ..., p_n\}$ be the set of distinct primes dividing $|G|$. For each i, let G_i be the Sylow p_i-group of G and $b_i = b\,|_{G_i\times G_i}$. Then*

$$(G,b) \cong (G_1,b_1) \perp ... \perp (G_n,b_n).$$

Proof. Since $G \cong \bigoplus G_i$, for $g, h \in G$ and each i there exists unique $g_i, h_i \in G_i$ such that $g = \sum g_i$ and $h = \sum h_i$. Then

$$b(g,h) = b\left(\sum_i g_i, \sum_j h_j\right) = \sum_{i,j} b(g_i,h_j).$$

However, if p and q are distinct primes, then there exists integers r and s such that $pr+qs = 1$. Thus if $i \neq j$

$$b(g_i,h_j) = (p_ir + p_js)b(g_i,h_j) = b(p_ir \cdot g_i, h_j) + b(g_i, p_js \cdot h_j) = 0$$

Thus $b(g,h) = \sum b_i(g_i,h_i)$ which implies $(G,b) \cong (G_i,b_i) \perp ... \perp (G_n,b_n)$. □

Definition 2.2.2. Let R be a commutative ring with 1. Let E_{ij} be the $n \times n$ matrix over R whose (i,j)-th entry is 1 and all other entries are 0. Let I_n denote the $n \times n$ identity matrix over R. Let A be an $n \times n$ matrix with entries in some R-module M. A *row-column operation* on A is one of the following operations:

- Let $\mathrm{Flip}_{i,j}(A) = S^{\mathrm{tr}}TS$ where $S = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$. This operation interchanges the i-th and j-th row of A and then interchanges the i-th and j-th column of A.
- Let $\mathrm{Add}_i^{r,j}(A) = S^{\mathrm{tr}}TS$ where $S = I_n + rE_{ji}$ for some $r \in R$ and $i \neq j$. This operation adds r times the j-th row to the i-th row of A and then adds r times the j-th column to the i-th column of A.
- Let $\mathrm{Scale}_i^r(A) = S^{\mathrm{tr}}AS$ for $S = I_n + (r-1)E_{ii}$ for some $r \in R$. This operation multiplies the i-th row of A by r and multiplies the i-th column of A by r.
- Let B be a gram matrix of a discriminant form (G, b) for a given set of generators $e_1, ..., e_n \in G$. Let O be a row-column operation on B. We say that O is *valid* if and only if the matrix $S = ((s_{ij}))$ such that $S^{\mathrm{tr}}BS = O(B)$ induces an automorphism of G by mapping $e_i \mapsto \sum_j s_{ij}e_j$ for all i.

Lemma 2.2.3. *Let b be a bilinear form on a finite abelian p-group G. If $g \in G$, then $v_p(g) \leq v_p(b(g,h))$ for all $h \in G$. Further, if b is non-degenerate, then $v_p(g) = \min\{v_p(b(g,h)) : h \in G\}$.*

Proof. Let $m = \max\{-v_p(b(g,h)) : h \in G\}$. Let $r = -v_p(g)$. Then

$$p^r b(g,h) = b(p^r g, h) = b(0,h) = 0 \quad \text{for all } h \in G.$$

So $r \geq -v_p(b(g,h))$ for all $h \in G$, which implies $r \geq m$. Now assume b is non-degenerate. For each $h \in G$, since $b(g,h) \in \mathbb{Q}_{(p)}/\mathbb{Z}$ and $-v_p(b(g,h)) \leq m$ we have $0 = p^m b(g,h) = b(p^m g, h)$ for all $h \in G$. Since b is non-degenerate, it follows that $p^m g = 0$, so $r \leq m$. □

Lemma 2.2.4. *Let G be a finite abelian group, and let $e_1, ..., e_n \in G$ such that $G = \oplus_{i=1}^n \langle e_i \rangle$. Let i and j be positive integers less than or equal to n, and let f be the homomorphism induced by mapping $e_i \mapsto e_i + re_j$ where r is an integer such that* $\mathrm{order}(re_j)$ *divides* $\mathrm{order}(e_i)$ *as well as mapping $e_k \mapsto e_k$ for all $k \neq i$. Then f is an automorphism of G.*

Proof. We must check that f is well defined and invertible. By assumption, for all k, $\text{order}(f(e_k)) = \text{order}(e_k)$. For all k, since $\langle e_k \rangle$ is cyclic, there exists a homomorphism $f_k : \langle e_k \rangle \to G$ such that $f_k(e_k) = f(e_k)$. By the universal property of the direct sum, $f : G \to G$ is a well-defined homomorphism. Since the $\{f(e_1), ..., f(e_n)\}$ generate G, and since G is finite, f is an automorphism of G. □

Lemma 2.2.5. *Let p be an odd prime. Let u_p be a quadratic non-residue modulo p. Let $A \neq 0$ be a symmetric matrix in $M_n(\mathbb{Q}_{(p)}/\mathbb{Z})$. Let r_1 be the smallest number such that $p^{r_1}A = 0$.*

(a) Then there exists a matrix $S \in \text{GL}_n(\mathbb{Z})$ such that $S \bmod p \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$ and

$$S^{tr}AS = \text{diag}(p^{-r_1}\epsilon_1, \cdots, p^{-r_n}\epsilon_n), \quad \text{with } r_1 \geq r_2 \geq \cdots \geq r_n \geq 0,\ \epsilon_j \in \{1, u_p, 0\}.$$

(b) Let G be a p group and b be a non-degenerate bilinear form on G. Let $G = \oplus_{j=1}^n \langle e_j \rangle$ and $A = \text{gram}_b(e_1, \cdots, e_n)$. Then there exists $f_1, \cdots, f_n \in G$ such that $G = \oplus_{j=1}^n \langle f_j \rangle$ and $\text{gram}_b(f_1, \cdots, f_n) = \text{diag}(p^{-r_1}\epsilon_1, \cdots, p^{-r_n}\epsilon_n)$ with $r_1 \geq r_2 \geq \cdots \geq r_n \geq 0$, $\epsilon_j \in \{1, u_p\}$.

Proof. (a) It is enough to find a sequence of row-column operations to diagonalize A. One proceeds as usual by finding a pivot with the smallest p-valuation and then using this pivot to sweep out the rows and columns.

Let $A = ((a_{ij})) \in M_n(\mathbb{Q}_{(p)}/\mathbb{Z})$ be a symmetric matrix. Let r_1 be the smallest integer such that $p^{r_1}A = 0$. Assume $r_1 > 0$. By induction on n, it suffices to show that there is a sequence of row-column operations that converts A to a matrix of the form $\left(\begin{smallmatrix} d_1 & 0 \\ 0 & A' \end{smallmatrix}\right)$ where $d_1 = p^{-r_1}$ or $d_1 = u_p p^{-r_1}$ and $A' \in M_{n-1}(\mathbb{Q}_{(p)}/\mathbb{Z})$ is a symmetric matrix such that $p^{r_1}A' = 0$.

Finding a pivot: *We claim that after changing A by row column operations, we may assume that $a_{11} = p^{-r_1}$ or $a_{11} = u_p p^{-r_1}$.*

proof of claim: If there is a diagonal entry a_{ii} such that $v_p(a_{ii}) = -r_1$, then apply Flip_{1i} to A to get $v_p(a_{11}) = -r_1$. Otherwise, there exists $i \neq j$ such that $v_p(a_{ij}) = -r_1$ and $v_p(a_{ii}) > -r_1, v_p(a_{jj}) > -r_1$. In this case, apply $\text{Add}_i^{j,1}$ to A. This changes the (i,i)-th entry of the matrix from a_{ii} to $(a_{ii}+2a_{ij}+a_{jj})$. By Lemma 2.1.3 parts (b) and (d) $v_p(a_{ii}+2a_{ij}+a_{jj}) = -r_1$. [1]. Now we apply Flip_{1i}. Either way we get $v_p(a_{11}) = -r_1$. Using the operation Scale_i^r we can change a_{11} to $r^2 a_{11}$. By choosing r appropriately, we can make $a_{11} = p^{-r_1}$ or $a_{11} = u_p p^{-r_1}$.

[1] this is the step in the argument that fails for $p = 2$ in some cases

Sweeping out: Now $a_{11} = \epsilon_1 p^{-r_1}$ with $\epsilon_1 = 1$ or u_p. Since ϵ_1 is relatively prime to p, we can pick $\epsilon' \in \mathbb{Z}$ such that $\epsilon_1\epsilon' \equiv 1 \bmod p^{r_1}$. We can represent a_{12} in the form β/p^{r_1} with $\beta \in \mathbb{Z}$. With the row-column operation $\mathrm{Add}_2^{1,-\epsilon'\beta}$ we add $(-\epsilon'\beta)$ times the first row to the second row and then add $(-\epsilon'\beta)$ times the first column to the second column to make $a_{12} = 0$ and $a_{21} = 0$. Similarly, we can make $a_{13} = a_{31} = 0$ and so on, thus converting A to a matrix of the form $\left(\begin{smallmatrix} \epsilon_1 p^{-r_1} & 0 \\ 0 & A' \end{smallmatrix}\right)$. Finally note that the entries of A' are $\mathbb{Z}$-linear combinations of entries of A, so $p^{r_1}A = 0$ implies $p^{r_1}A' = 0$. Notice that for each row-column operation O we used above, the matrix S such that $S^{\mathrm{tr}}AS = O(A)$ must have a determinant relatively prime to p. Thus, the product of these matrices modulo p is an element of $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Now part (a) follows by induction.

(b) Assume the setup of (b). part (a) shows that the matrix A can be diagonalized by a sequence of row-column operations. We need to verify that all the row-column operation used in the proof of part (a) are valid. Our use of Scale_i^r was valid since r was always relatively prime to p. In order to avoid an invalid row-column operation, whenever we would have used $\mathrm{Flip}_{i,j}$ in (a) simply re-order the generators $\mathrm{gram}_b(e_1, ..., e_n)$ to $\mathrm{gram}_b(f_1, ..., f_n)$ where $f_i = e_j$, $f_j = e_i$, and $f_k = e_k$ for $k \notin \{i, j\}$. Now one only has to check the operations $\mathrm{Add}_j^{r,i}$ are valid.

While finding the pivot, we may perform $\mathrm{Add}_i^{1,j}$ to a matrix $\mathrm{gram}(e_1, ...e_n)$ if a non-diagonal (i, j)-th entry of the matrix has the highest power of p in the denominator and further, all diagonal entries have strictly lower powers of p in the denominator. Since (G, b) is non-degenerate, Lemma 2.2.3 implies that $\mathrm{order}(e_i) = \mathrm{order}(e_j) = \exp(G)$. By Lemma 2.2.4 this row-column operation induces an automorphism on G. Hence $\mathrm{Add}_i^{1,j}$ is valid.

While sweeping out we also perform $\mathrm{Add}_i^{r,1}$ for all $i > 1$. We may assume $a_{1i} \neq 0$ or else no row-column operation need have been done in the first place. By Lemma 2.1.3 part (b) $v_p(r) = v_p(a_{1i}) + r_1$. By Lemma 2.2.3 $v_p(e_i) \leq v_p(a_{1i})$. Thus $\mathrm{order}(re_1) \leq \mathrm{order}(e_i)$. By Lemma 2.2.4 this row-column operation induces an automorphism on G. Hence $\mathrm{Add}_i^{r,1}$ is valid.

It follows that there exists $f_1, \cdots, f_n \in G$ such that $G = \oplus\langle f_j\rangle$ and $\mathrm{gram}_b(f_1, \cdots, f_n) = \mathrm{diag}(p^{-r_1}\epsilon_1, \cdots, p^{-r_n}\epsilon_n)$ with $r_1 \geq r_2 \geq \cdots \geq r_n \geq 0$, $\epsilon_j \in \{1, u_p, 0\}$. Since (G, b) it non-degenerate, it follows that we must have $\epsilon_j \neq 0$ and $\mathrm{order}(f_j) = p^{r_j}$ for all j. $\square$

Lemma 2.2.6. *(a) Let $A \neq 0$ be a symmetric matrix in $M_n(\mathbb{Q}_{(2)}/\mathbb{Z})$. Let m be the smallest number such that $2^m A = 0$. Then there exists a matrix $S \in \mathrm{GL}_n(\mathbb{Z})$ such that $(S \bmod 2) \in \mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z})$ and $S^{tr}AS$ is block diagonal with blocks of size 1 or 2. Each block is of the form*

$$\big(2^{-r}\delta\big), \quad \text{or} \quad 2^{-r}\left(\begin{smallmatrix} 2a & d \\ d & 2c \end{smallmatrix}\right) \tag{2.1}$$

where r is some non-negative integer, a, c, d are integers with d odd and $\delta \in \{0, \pm 1, \pm 5\}$. The largest r that shows up is equal to m.

(b) Let G be a finite abelian 2-group and b be a non-degenerate bilinear form on G. Let $G = \oplus_{j=1}^n \langle e_j \rangle$ and $A = \mathrm{gram}(e_1, \cdots, e_n)$. Then there exists $f_1, \cdots, f_n \in G$ such that $G = \oplus_{j=1}^n \langle f_j \rangle$ and $\mathrm{gram}_b(f_1, \cdots, f_n)$ is a block diagonal matrix with with blocks of size one or two. Each block is of the form given in (2.1) where r is some non-negative integer, a, b, c are integers with b odd and $\delta \in \{\pm 1, \pm 5\}$. The largest r that shows up is equal to m.

Proof. (a) As above, we try to get a diagonal entry of A to have minimum 2-valuation. If this succeeds, then we can proceed with the sweep out as before and split off a one-by-one block from A. This procedure fails only in the situation when none of the entries of A with minimal 2-valuation lie on the diagonal. Then there is a 2×2 block in A which has the form $2^{-m}\left(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}\right)$ with $\alpha, \beta, \gamma \in \mathbb{Z}$, β odd and all the diagonal entries of A have 2 valuation strictly larger than $-m$. In this case, we can use Flip_{ij}'s to move this 2×2 sub-matrix to the upper left corner of A so that $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) = 2^{-m}\left(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}\right)$ and then use this 2×2 block to sweep out the first two rows and first two columns simultaneously.

This is how it is done: Suppose the first two entries of the i-th row are $2^{-m}(u, v)$ for $u, v \in \mathbb{Z}$ where $i > 2$. We want to find r_1, r_2 such that

$$(r_1, r_2) 2^{-m}\left(\begin{smallmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{smallmatrix}\right) = -2^{-m}(u, v).$$

This system can always be solved since the determinant $(4\alpha\gamma - \beta^2)$ of the coefficient matrix is odd. Solving the equation yields yields

$$(r_1, r_2) = -h(2\gamma u - \beta v, 2\alpha v - \beta u)$$

where h is an inverse of $(4\alpha\gamma - \beta^2)$ modulo 2^m. Perform $\mathrm{Add}_i^{r_1,1}$ and $\mathrm{Add}_i^{r_2,2}$. Verify that after this operation the first two entries of the i-th row and i-th column become zero. This proves part (a).

(b) Again, we must check that all row-column operations used above were valid. Because of Lemma 2.2.5 (b), it is only necessary to prove that row-column operations were valid in the case when there were no diagonal entries of A with minimal 2-valuation. The sweep out operation described in part (a) above corresponds to replacing $\mathrm{gram}(e_1, \cdots, e_n)$ by $\mathrm{gram}(f_1, \cdots, f_n)$ where $f_i = e_i + r_1 e_1 + r_2 e_2$ and $f_j = e_j$ for all $j \neq i$. Note that since 2^m is the maximum denominator in A and b is non-degenerate, $\mathrm{order}(e_1) = \mathrm{order}(e_2) = 2^m$. Suppose order $e_i = 2^k$. Then u and v must be divisible by 2^{m-k} because the entries of the i-th row can have denominator at most 2^k. From the formula for r_1 and r_2 we see that 2^{m-k} divides r_1 and r_2. It follows that $2^k f_i = 0$. On the other hand since $\langle e_i \rangle \cap \langle e_1, e_2 \rangle = 0$, we have $\mathrm{order}(f_i) \geq 2^k$. So $\mathrm{order}(f_i) = \mathrm{order}(e_i)$ By Lemma 2.2.4 this row-column operation induces an automorphism on G. Hence the sweep out operations using 2×2 blocked above are valid. □

Lemma 2.2.7. *(a) Let s be a 2×2 matrix of indeterminates. Let*

$$(A(s), B(s), C(s)) = (s_{11}^2 + s_{11}s_{12} + s_{12}^2, 2s_{11}s_{21} + s_{11}s_{22} + s_{21}s_{12} + 2s_{12}s_{22}, s_{21}^2 + s_{21}s_{22} + s_{22}^2).$$

Let A, B, C be odd integers. Let $n \geq 1$. Then the equation

$$(A(s), B(s), C(s)) \equiv (A, B, C) \bmod 2^n. \tag{2.2}$$

has a solution $S \in M_2(\mathbb{Z})$ such that $S \equiv I \bmod 2$.

(b)Let s be a 2×2 matrix of indeterminates. Let

$$(A(s), B(s), C(s)) = (s_{11}s_{12}, s_{11}s_{22} + s_{21}s_{12}, s_{21}s_{22}).$$

Let A, B, C be integers such that B is odd and AC is even. Let $n \geq 1$. Then the equation

$$(A(s), B(s), C(s)) \equiv (A, B, C) \bmod 2^n. \tag{2.3}$$

has a solution $S \in M_2(\mathbb{Z})$ such that $S \equiv \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right) \bmod 2$.

Proof. (a) We induct on n. Observe that, $S = I$ is a solution to equation (2.2) for $n = 1$ since A, B, C are odd. By induction, suppose we have found $s = \left(\begin{smallmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{smallmatrix}\right)$ such that $s \equiv I \bmod 2$ and s is a solution to equation (2.2) for $n \leq m$. Then there exists $A', B', C' \in \{0, 1\}$ such that

$$(A(s), B(s), C(s)) \equiv (A + 2^m A', B + 2^m B', C + 2^m C') \bmod 2^{m+1}.$$

Let $\tilde{s}_{ij}$ be an integer such that $\tilde{s}_{ij} \equiv s_{ij} \bmod 2^m$. Then $\tilde{s}_{ij} \equiv s_{ij} + 2^n \epsilon_{ij} \bmod 2^{m+1}$ for $\epsilon_{ij} \in \{0, 1\}$. Let $\tilde{s} = (\!(\tilde{s}_{ij})\!)$. Now we calculate:

$$\begin{aligned} A(\tilde{s}) &\equiv A + 2^m(A' + s_{11}\epsilon_{12} + s_{12}\epsilon_{11}) \bmod 2^{m+1}, \\ B(\tilde{s}) &\equiv B + 2^m(B' + s_{11}\epsilon_{22} + s_{22}\epsilon_{11} + s_{12}\epsilon_{21} + s_{21}\epsilon_{12}) \bmod 2^{m+1}, \\ C(\tilde{s}) &\equiv C + 2^m(C' + s_{22}\epsilon_{21} + s_{21}\epsilon_{22}) \bmod 2^{m+1}. \end{aligned}$$

So $\tilde{s}$ is a solution to equation (2.2) for $n = m + 1$ if and only if the equation (2.4) below has a solution:

$$\begin{pmatrix} s_{12} & 0 & s_{11} & 0 \\ s_{22} & s_{12} & s_{21} & s_{11} \\ 0 & s_{22} & 0 & s_{21} \end{pmatrix} \begin{pmatrix} \epsilon_{11} \\ \epsilon_{21} \\ \epsilon_{12} \\ \epsilon_{22} \end{pmatrix} \equiv \begin{pmatrix} A' \\ B' \\ C' \end{pmatrix} \bmod 2. \tag{2.4}$$

Since $s \equiv I \bmod 2$, we have

$$\begin{pmatrix} s_{12} & 0 & s_{11} & 0 \\ s_{22} & s_{12} & s_{21} & s_{11} \\ 0 & s_{22} & 0 & s_{21} \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \bmod 2.$$

This matrix has rank 3 over $\mathbb{F}_2$, so equation (2.4) has a solution. This proves part (a).

(b) The proof of part (b) is similar and easier. Observe that, $S = \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right)$ is a solution to our congruences for $n = 1$ since AC is even and B is odd. The induction step then proceeds exactly as in the proof of part (a). By induction, suppose we have found $s = \left(\begin{smallmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{smallmatrix}\right)$ such that $s \equiv \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right) \bmod 2$ and s is a solution to equation (2.3) for integers $n \leq m$. Then there exists $A', B', C' \in \{0, 1\}$ such that

$$(A(s), B(s), C(s)) \equiv (A + 2^m A', B + 2^m B', C + 2^m C') \bmod 2^{m+1}.$$

Let $\tilde{s} = ((\tilde{s}_{ij}))$ where $\tilde{s}_{ij} \equiv s_{ij} + 2^n \epsilon_{ij} \bmod 2^{m+1}$ for $\epsilon_{ij} \in \{0,1\}$. Again we find that $\tilde{s}$ is a solution to equation (2.3) for $n = m+1$ if and only if the equation (2.4) has a solution. Since $s \equiv \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right) \bmod 2$, we have

$$\begin{pmatrix} s_{12} & 0 & s_{11} & 0 \\ s_{22} & s_{12} & s_{21} & s_{11} \\ 0 & s_{22} & 0 & s_{21} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & A & 0 \\ C & 1 & 1 & A \\ 0 & C & 0 & 1 \end{pmatrix} \bmod 2.$$

Since A or C is even, either the second or the third column of the above matrix is equal to $(0,1,0)^{tr}$. So the matrix has rank 3, and thus equation (2.4) has solutions. □

Lemma 2.2.8. *Let q be an irreducible non-degenerate quadratic form on $G = (\mathbb{Z}/2^r\mathbb{Z})^2$. Then there exists $A, B, C \in \mathbb{Z}$ with B odd such that $q(x) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2)$. If AC is even, then $(G,q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, x_1x_2/2^r)$. Otherwise $(G,q) \simeq ((\mathbb{Z}/2^r\mathbb{Z})^2, (x_1^2 + x_1x_2 + x_2^2)/2^r)$.*

Proof. (a) Note that $2q(x) = b_q(x,x) \in 2^{-r}\mathbb{Z}/\mathbb{Z}$. So $q(x)$ takes values in $2^{-r-1}\mathbb{Z}/\mathbb{Z}$. So

$$q(x_1,x_2) = 2^{-r-1}(\alpha x_1^2 + 2Bx_1x_2 + \gamma x_2^2)$$

where $q(1,0) = 2^{-r-1}\alpha$, $q(0,1) = 2^{-r-1}\gamma$ and $b_q((1,0),(0,1)) = 2^{-r}B$. Suppose α is odd. Let $\bar{\alpha}$ be an inverse of α modulo 2^{r+1}. Then we can complete squares to write

$$q(x_1,x_2) = 2^{-r-1}(\alpha(x_1 + B\bar{\alpha}x_2)^2 + (\gamma - B^2\bar{\alpha})x_2^2).$$

This contradicts the irreducibility of q. So α has to be even. For the same reason γ has to be even. So we can write

$$q(x_1,x_2) = 2^{-r}(Ax_1^2 + Bx_1x_2 + Cx_2^2).$$

If A, B, C are all even, then b_q takes values in $2^{-r+1}\mathbb{Z}/\mathbb{Z}$ and hence cannot be non-degenerate. If B is even, then A or C must be odd, and we can once again complete squares (as above) and decompose (G,q) into orthogonal direct sum of two metric groups. So B must be odd.

First, suppose AC is odd. Let $F(x_1,x_2) = x_1^2 + x_1x_2 + x_2^2$. Note that

$$F((x_1,x_2)S) = A(S)x_1^2 + B(S)x_1x_2 + C(S)x_2^2$$

where $(A(s), B(s), C(s))$ are the polynomials given in 2.2.7(a). We want to show $q(x_1, x_2) \simeq 2^{-r}F(x_1, x_2)$. This is equivalent to finding a matrix $S \in M_2(\mathbb{Z})$ with odd determinant such that

$$F((x_1, x_2)S) \equiv (Ax_1^2 + Bx_1x_2 + Cx_2^2) \bmod 2^n,$$

or equivalently, $(A(S), B(S), C(S)) \equiv (A, B, C) \bmod 2^n$. So the lemma follows from 2.2.7(a), if AC is odd. If AC is even, then the proof is identical, using $F(x_1, x_2) = x_1x_2$ and using part (b) of 2.2.7 instead of part (a). □

Lemma 2.2.9. *(a) Let A, B, C be odd integers. Let $r \geq 1$. Then there exists a matrix $S \in M_2(\mathbb{Z})$ such that $S^{tr}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)S \equiv \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right) \bmod 2^r$ and $S \equiv I \bmod 2$.*

(b) Let A, B, C be integers such that AC is odd and B is even. Let $r \geq 1$. Then there exists a matrix $S \in M_2(\mathbb{Z})$ such that $S^{tr}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)S \equiv \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right) \bmod 2^r$ and $S \equiv \left(\begin{smallmatrix} A & 1 \\ 1 & C \end{smallmatrix}\right) \bmod 2$.

Proof. (a) The congruences in part (a) translate into $A(s) \equiv A \bmod 2^{r-1}, B(s) \equiv B \bmod 2^r, C(s) = C \bmod 2^{r-1}$ where $A(s), B(s), C(s)$ are as in 2.2.7 (a). Part (a) thus follows from 2.2.7. Similarly part (b) follows from part (b) of 2.2.7. □

Theorem 2.2.10 ([21])**.** *(a) Each non-degenerate discriminant form is an orthogonal direct sum of the irreducible discriminant forms listed in Table 2.1.*

(b) Each metric group is an orthogonal direct sum of the irreducible metric groups listed in Table 2.1.

Proof. (a) Let (G, b) be a non-degenerate discriminant form. By Lemma 2.2.1 it suffices to decompose (G, b) into irreducibles when G is a p-group for some prime p. First suppose p is odd.

From Lemma 2.2.5, It follows that there exists $f_1, \cdots, f_n \in G$ such that $G = \oplus\langle f_j\rangle$ and $\text{gram}_b(f_1, \cdots, f_n) = \text{diag}(p^{-r_1}\epsilon_1, \cdots, p^{-r_n}\epsilon_n)$ with $r_1 \geq r_2 \geq \cdots \geq r_n \geq 0$, $\epsilon_j \in \{1, u_p\}$. Recall that u_p is a quadratic non-residue modulo p. Since (G, b) it non-degenerate, it follows that we must have $\text{order}(f_j) = p^{r_j}$ for all j. Thus (G, b) is orthogonal direct sum of the rank one discriminant forms $(\langle f_j\rangle, b|_{\langle f_j\rangle})$ and each of these are of type A or B. This completes the argument for odd p.

Now we consider the case $p = 2$. From Lemma 2.2.6, it follows that there exists $f_1, \cdots, f_n \in G$ such that $G = \oplus\langle f_j\rangle$ and $\text{gram}_b(f_1, \cdots, f_n)$ is block diagonal with blocks of size one or two as given in Lemma 2.2.6. Accordingly (G, b) is an orthogonal direct sum of rank one or two discriminant forms spanned by one or two of the f_j's. The rank one forms among these are clearly of type A, B, C or D. The gram matrix of a rank two piece has the form $2^{-r}\left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$. Lemma 2.2.9 shows that such a rank two piece is either of type E or F.

(b) Now let (G, q) be a metric group. By part (a) (G, b_q) is an orthogonal direct sum of irreducible forms (G_j, b_j). Each G_j is a homogeneous p-group of rank 1 or 2. Further G_j can have rank two only if $p = 2$. It follows that (G, q) is also an orthogonal direct sum of (G_j, q_j) where $q_j = q|_{G_j}$. The rank one forms are clearly of type A, B, C or D. The rank two forms either decompose into two rank one forms or they are irreducible as metric groups. In the later case 2.2.8 shows that (G_j, q_j) is of type E or F. □

Lemma 2.2.11. *For p an odd prime and r a positive integer we have*

$$A_{p^r} \perp A_{p^r} \cong B_{p^r} \perp B_{p^r}$$

in the case of discriminant forms as well as pre-metric groups.

Proof. Let $(G, q) = A_{p^r} \perp A_{p^r}$ and $(H, w) = B_{p^r} \perp B_{p^r}$. Without loss of generality, let u be the smallest integer in $\{2, 3, ..., p-1\}$ that represents a quadratic non-residue mod p. Then there exists an integer a such that $a^2 \equiv u - 1 \mod p^r$. Let $f : G \to H$ be defined by $f(x, y) = (ax - y, x + ay)$. One checks that f is a group isomorphism. Also

$$\begin{aligned} q \circ f(x, y) &= q(ax - y, x + ay) \\ &= (ax - y)^2 + (x + ay)^2 \\ &= (a^2 + 1)x^2 + (a^2 + 1)y^2 \\ &= ux^2 + uy^2 \\ &= w(x, y). \end{aligned}$$

Thus $f : (G, q) \to (H, w)$ is a pre-metric isomorphism. Remark 2.1.11 implies the statement also holds for discriminant forms. □

2.3 Larger Pre-Metric Groups from Smaller Ones

Definition 2.3.1. Let (G, q) be a pre-metric group. Let (G, b_q) be the corresponding discriminant form. Let $M = ((m_{i,j}))$ be an $n \times n$ symmetric matrix over $\mathbb{Z}$. Then define a function $(M \otimes b_q) : G^n \times G^n \to \mathbb{Q}/\mathbb{Z}$ by

$$(M \otimes b_q)\Big((g_1, ..., g_n), (h_1, ..., h_n)\Big) = \sum_{i,j} m_{i,j} b_q(g_i, h_j). \tag{2.5}$$

And also define the function $(M \otimes q) : G^n \to \mathbb{Q}/\mathbb{Z}$ by

$$(M \otimes q)(g_1, ..., g_n) = \sum_i m_{i,i} q(g_i) + \sum_{i<j} m_{i,j} b_q(g_i, g_j). \tag{2.6}$$

Lemma 2.3.2. *Let (G, q) be a pre-metric group with corresponding discriminant form (G, b_q). Let $M = (m_{i,j})$ be an $n \times n$ symmetric matrix over $\mathbb{Z}$. Then $(G^n, M \otimes b_q)$ is a discriminant form and $(G^n, M \otimes q)$ is a pre-metric group whose corresponding discriminant form is $(G^n, M \otimes b_q)$.*

Proof. To prove that $(G^n, M \otimes b_q)$ is a discriminant form it is enough to see that since b_q is bilinear and M is symmetric $(M \otimes b_q)$ must also be bilinear.

Let $\overline{g}, \overline{h} \in G^n$ such that $\overline{g} = (g_1, ...g_n)$ and $\overline{h} = (h_1, ..., h_n)$. To show that $(M \otimes q)$ is a quadratic form such that $(M \otimes b_q)$ is the corresponding bilinear form it is enough to show that $(M \otimes q)(\overline{g} + \overline{h}) - (M \otimes q)(\overline{g}) - (M \otimes q))(\overline{h}) = (M \otimes b_q)(\overline{g}, \overline{h})$ and $(M \otimes q)(\overline{g}) = (M \otimes q)(-\overline{g})$. Now

$$\begin{aligned}
(M \otimes q)(\overline{g} + \overline{h}) - (M \otimes q)(\overline{g}) - (M \otimes q)(\overline{h}) &= \left(\sum_i m_{i,i} q(g_i + h_i) + \sum_{i<j} m_{i,j} b_q(g_i + h_i, g_j + h_j) \right) \\
&\quad - \left(\sum_i m_{i,i} q(g_i) + \sum_{i<j} m_{i,j} b_q(g_i, g_j) \right) \\
&\quad - \left(\sum_i m_{i,i} q(h_i) + \sum_{i<j} m_{i,j} b_q(h_i, h_j) \right) \\
&= \sum_i m_{i,i} b_q(g_i, h_i) + \sum_{i<j} 2 m_{i,j} b_q(g_i, h_j) \\
&= (M \otimes b_q)(\overline{g}, \overline{h})
\end{aligned}$$

as well as

$$\begin{aligned}(M \otimes q)(-\overline{g}) &= \sum_i m_{i,i} q(-g_i) + \sum_{i<j} m_{i,j} b_q(-g_i, -g_j) \\ &= \sum_i m_{i,i} q(g_i) + \sum_{i<j} m_{i,j} b_q(g_i, g_j) \\ &= (M \otimes q)(\overline{g})\end{aligned}$$

This proves the lemma. □

Lemma 2.3.3. *Let (G, q), (H, μ), (L, γ) be metric groups such that*

$$(G, q) = (H, \mu) \perp (L, \gamma).$$

Let M be an $n \times n$ symmetric integer matrix. Then

$$(G^n, M \otimes q) = (H^n, M \otimes \mu) \perp (L^n, M \otimes \gamma).$$

Proof. Let $(g_1, ..., g_n) \in G^n$. For each i, write $g_i = h_i + l_i$ with $h_i \in H$ and $l_i \in L$. Now

$$\begin{aligned}b_q(g_i, g_j) &= q(g_i + g_j) - q(g_i) - q(g_j) \\ &= \mu(h_i + h_j) + \gamma(l_i + l_j) - \mu(h_i) - \gamma(l_i) - \mu(h_j) - \gamma(l_j) \\ &= b_\mu(h_i, h_j) + b_\gamma(l_i, l_j).\end{aligned}$$

One has

$$\begin{aligned}M \otimes q(g_1, ..., g_n) &= \sum_i m_{ii} q(g_i) + \sum_{i<j} m_{ij} b_q(g_i, g_j) \\ &= \sum_i m_{ii}(\mu(h_i) + \gamma(l_i)) + \sum_{i<j} m_{ij}(b_\mu(h_i, h_j) + b_\gamma(l_i, l_j)) \\ &= M \otimes \mu(h_1, ..., h_n) + M \otimes \gamma(l_1, ..., l_n).\end{aligned}$$

This proves the lemma. □

Lemma 2.3.4. *Let (G, q) be a pre-metric p-group for some prime p. Let $S, M \in M_n(\mathbb{Z})$ such that M is symmetric and $S \mod p \in GL_n(\mathbb{Z}/p\mathbb{Z})$. Then $(G, M \otimes q) \cong (G, S^T M S \otimes q)$ is a pre-metric isomorphism.*

Proof. Since $(S \mod p) \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, $d = \det(S)$ is relatively prime to p. Let p^e be the exponent of G. Then there exists a $d' \in \mathbb{Z}$ such that $d'd \equiv 1 \mod p^e$. Let $T = d' \cdot \mathrm{adjugate}(S)$. Then T defines a map from G^n to G^n which is the inverse to S.

What is left is to prove that for all $(g_1, ..., g_n) \in G^n$ one has the following equality in $\mathbb{Q}/\mathbb{Z}$:

$$(M \otimes q)(S(g_1, ..., g_n)^{\mathrm{tr}}) = (S^{\mathrm{tr}} M S \otimes q)((g_1, ..., g_n)^{\mathrm{tr}}). \tag{2.7}$$

Since q is quadratic and b_q is bilinear and $b_q(g_i, g_i) = 2q(g_i)$ for i the left hand side of equation (2.7) is seen to be equal to

$$\sum_i m_{ii} q\left(\sum_k s_{ik} g_k\right) + \sum_{i<j} m_{ij} b_q\left(\sum_k s_{ik} g_k, \sum_l s_{jl} g_l\right)$$
$$= \sum_i m_{ii}\left(\sum_k s_{ik}^2 q(g_k) + \sum_{k<l} s_{ik} s_{il} b_q(g_k, g_l)\right) + \sum_{i<j} m_{ij}\left(\sum_{k\neq l} s_{ik} s_{jl} b_q(g_k, g_l) + \sum_k s_{ik} s_{jk} 2q(g_k)\right)$$

Since $b_q(g_k, g_l) = b_q(g_l, g_k)$, the last expression above can be written in the form

$$\sum_k \alpha_{kk} q(g_k) + \sum_{k<l} \alpha_{kl} b_q(g_k, g_l) \quad \text{for some coefficients } \alpha_{kl}$$

It remains to collect together terms and verify that $\alpha_{kl} = (S^{\mathrm{tr}} T S)_{kl}$. One has

$$\alpha_{kk} = \sum_i m_{ii} s_{ik}^2 + 2\sum_{i<j} m_{ij} s_{ik} s_{jk} = (S^{\mathrm{tr}} T S)_{kk}$$

Let $k < l$. Then

$$\alpha_{kl} = \sum_i m_{ii} s_{ik} s_{il} + \sum_{i<j} m_{ij} s_{ik} s_{jl} + \sum_{i<j} m_{ij} s_{ik} s_{il} + \sum_{i\neq j} m_{ij} s_{il} s_{jk} = (S^{\mathrm{tr}} T S)_{kl}.$$

where the second equality follows by interchanging i and j in the sum $\sum_{i<j} m_{ij} s_{il} s_{jk}$ and remembering that $m_{ij} = m_{ji}$. □

Lemma 2.3.5. *Let (G, q) be a pre-metric p-group for a prime p. Let $m = \max\{-v_p(q(g)) : g \in G\}$. Let $M = ((m_{i,j})), A = ((a_{i,j})) \in M_n(\mathbb{Z})$ such that $M \equiv A \mod p^m$. Then $(G^n, M \otimes q) = (G^n, A \otimes q)$.*

Proof. Let $\overline{g} \in G^n$ such that $\overline{g} = (g_1, ..., g_n)$. Then

$$\begin{aligned} M \otimes q(\overline{g}) &= \sum_{i=1}^{n} m_{i,i} q(g_i) + \sum_{i<j} m_{i,j} b_q(g_i, g_j) \mod \mathbb{Z} \\ &= \sum_{i=1}^{n} a_{i,i} q(g_i) + \sum_{i<j} a_{i,j} b_q(g_i, g_j) \mod \mathbb{Z} \\ &= A \otimes q(\overline{g}). \end{aligned}$$

□

2.4 Quadratic Gauss Sums

Theorem 2.4.1 ([4] p. 50)**.** *For p an odd prime, k a positive integer, and α an integer relatively prime to p, the values of the quadratic Gauss sum is given by*

$$\sum_{x=1}^{p^k} \mathbf{e}\left(\frac{\alpha x^2}{p^k}\right) = \left(\frac{\alpha}{p}\right)^k (-1)^{k(p^2-1)/8} p^{k/2}$$

where $\left(\text{-}\right)$ is the Legendre symbol.

Definition 2.4.2. Let (G, q) be a pre-metric group. Define

$$\Theta(G, q) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \mathbf{e}\left(q(x)\right).$$

One can see that if $(G, q) \cong (H, w)$, then $\Theta(G, q) = \Theta(H, w)$, and if (G, q) is an orthogonal direct sum of (G_1, q_1) and (G_2, q_2), then $\Theta(G, q) = \Theta(G_1, q_1)\Theta(G_2, q_2)$.

Corollary 2.4.3. *Let p be an odd prime and let u be a quadratic non-residue of $\mathbb{Z}/p\mathbb{Z}$. Let r be a positive integer, and let $\alpha \in \{1, u\}$. Then*

$$\Theta\left(\mathbb{Z}/p^r\mathbb{Z}, \frac{\alpha(p^r+1)x^2}{2p^r}\right) = \left(\frac{2\alpha}{p}\right)^r (-1)^{r(p^2-1)/8}$$

where $\left(\text{-}\right)$ is the Legendre symbol.

Lemma 2.4.4. *Let r be a positive integer. If $r = 1$, let $\alpha \in \{1, -1\}$. If $r \geq 2$, let $\alpha \in \{1, -1, 5, -5\}$. Then*

$$\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{\alpha x^2}{2^{r+1}}\right) = (-1)^{r(\alpha^2-1)/8} \mathbf{e}\left(\frac{\alpha}{8}\right)$$

Proof. The proof is inductive. Consider

$$\begin{aligned}\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{\alpha x^2}{2^{r+1}}\right) &= \frac{1}{\sqrt{2^r}} \sum_{x=0}^{2^r-1} \mathbf{e}\left(\frac{\alpha x^2}{2^{r+1}}\right) \\ &= \frac{1}{2\sqrt{2^r}} \sum_{x=0}^{2^r-1} \mathbf{e}\left(\frac{\alpha x^2}{2^{r+1}}\right) + \frac{1}{2\sqrt{2^r}} \sum_{x=0}^{2^r-1} \mathbf{e}\left(\frac{\alpha (x+2^r)^2}{2^{r+1}}\right) \\ &= \frac{1}{2\sqrt{2^r}} \sum_{x=0}^{2^{r+1}-1} \mathbf{e}\left(\frac{\alpha x^2}{2^{r+1}}\right)\end{aligned}$$

However, when $r \geq 4$ we may split the sum above

$$\begin{aligned}\sum_{x=0}^{2^{r+1}-1} \mathbf{e}\left(\frac{\alpha x^2}{2^{r+1}}\right) &= \sum_{x=0}^{2^{r-1}-1} \sum_{y=0}^{1} \sum_{z=0}^{1} \mathbf{e}\left(\frac{\alpha(2^r y + 2x + z)^2}{2^{r+1}}\right) \\ &= 2 \sum_{x=0}^{2^{r+1}-1} \sum_{z=0}^{1} \mathbf{e}\left(\frac{\alpha(4x^2 + 4xz + z^2)}{2^{r+1}}\right) \\ &= 2 \sum_{x=0}^{2^{r-1}-1} \mathbf{e}\left(\frac{\alpha x^2}{2^{r-1}}\right) + 2 \sum_{x=0}^{2^{r-1}-1} \mathbf{e}\left(\frac{\alpha(4x^2 + 4x + 1)}{2^{r+1}}\right).\end{aligned}$$

The second sum above is equal to zero since

$$\begin{aligned}\sum_{x=0}^{2^{r-1}-1} \mathbf{e}\left(\frac{\alpha(4x^2 + 4x + 1)}{2^{r+1}}\right) &= \mathbf{e}\left(\frac{\alpha}{2^{r+1}}\right) \sum_{x=0}^{2^{r-2}-1} \sum_{y=0}^{1} \mathbf{e}\left(\frac{\alpha(x + 2^{r-2}y)^2 + \alpha(x + 2^{r-2}y)}{2^{r-1}}\right) \\ &= \mathbf{e}\left(\frac{\alpha}{2^{r+1}}\right) \sum_{x=0}^{2^{r-2}-1} \mathbf{e}\left(\frac{\alpha(x^2 + x)}{2^{r-1}}\right) \sum_{y=0}^{1} (-1)^y \\ &= 0\end{aligned}$$

Thus, for $r \geq 4$

$$\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{\alpha x^2}{2^{r+1}}\right) = 2\Theta\left(\mathbb{Z}/2^{r-2}\mathbb{Z}, \frac{\alpha x^2}{2^{r-1}}\right).$$

By checking base cases for $r = 1, 2, 3$ and appropriate α the lemma is proven. □

Lemma 2.4.5. *Let r be a positive integer and let $\alpha \in \{0, 1\}$. Let*

$$(G, q) = \left((\mathbb{Z}/2^r\mathbb{Z})^2, \frac{\alpha x_1^2 + x_1 x_2 + \alpha x_2^2}{2^r}\right).$$

Then

$$\Theta(G, q) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \mathbf{e}(q(g)) = (-1)^{\alpha r}$$

Proof. For $r = 1, 2$ check the formula directly. For $n \geq 3$ we have

$$\Theta(G,q) = \sum_{x,y=1}^{2^r} \mathbf{e}\left(\frac{\alpha x^2 + xy + \alpha y^2}{2^r}\right) = \sum_{x_0,y_0=1}^{2^{r-1}} \mathbf{e}\left(\frac{\alpha x_0^2 + \alpha y_0^2}{2^r}\right) \sum_{(x,y)=(x_0,y_0) \mod 2^{r-1}} \mathbf{e}\left(\frac{xy}{2^r}\right)$$

The inner sum is equal to

$$\mathbf{e}\left(\frac{x_0 y_0}{2^r}\right)\left(1+\mathbf{e}\left(\frac{x_0}{2}\right)\right)\left(1+\mathbf{e}\left(\frac{y_0}{2}\right)\right) = \begin{cases} 4\mathbf{e}\left(\frac{x_0y_0}{2^r}\right) & \text{if } x_0 \equiv y_0 \equiv 0 \mod 2 \\ 0 & \text{otherwise} \end{cases}$$

This implies

$$\begin{aligned}\Theta(G,q) &= 4 \sum_{\substack{x_0,y_0=1 \\ x_0,y_0 \equiv 0 \mod 2}}^{2^{r-1}} \mathbf{e}\left(\frac{\alpha x_0^2 + x_0y_0 + \alpha y_0^2}{2^r}\right) \\ &= 4 \sum_{x_0,y_0=1}^{2^{r-2}} \mathbf{e}\left(\frac{\alpha x_0^2 + x_0y_0 + \alpha y_0^2}{2^{r-2}}\right) \\ &= 4\Theta\left((\mathbb{Z}/p^{r-2}\mathbb{Z})^2, \frac{\alpha x_1^2 + x_1x_2 + \alpha x_2^2}{2^{r-2}}\right)\end{aligned}$$

The lemma follows inductively. □

Lemma 2.4.6. *Let p be an odd prime, and let u be a quadratic non-residue of $\mathbb{Z}/p\mathbb{Z}$. Let r be a positive integer and let s be an integer such that $0 \leq s \leq r$. Let $\alpha \in \{1, u\}$. Let $(G, q_1) = A_{p^r}$ and $(G, q_u) = B_{p^r}$. Then*

$$\Theta(G, \alpha p^s \cdot q_1) = (-1)^{r-s}\Theta(G, \alpha p^s \cdot q_u)$$

Proof. Let $\beta \in \{1, u\}$. Then

$$\begin{aligned}\Theta(G, \alpha p^s q_\beta) &= \frac{1}{\sqrt{p^r}} \sum_{x=1}^{p^r} \mathbf{e}\left(\frac{\alpha\beta(p^r+1)x^2}{2p^{r-s}}\right) \\ &= \frac{1}{\sqrt{p^r}} \sum_{x=1}^{p^{r-s}} \sum_{y=1}^{p^s} \mathbf{e}\left(\frac{\alpha\beta(p^{r-s}+1)(x+p^{r-s}y)^2}{2p^{r-s}}\right) \\ &= \frac{\sqrt{p^s}}{\sqrt{p^{r-s}}} \sum_{x=1}^{p^{r-s}} \mathbf{e}\left(\frac{\alpha\beta(p^{r-s}+1)x^2}{2p^{r-s}}\right) \\ &= \sqrt{p^s}\Theta\left(\mathbb{Z}/p^{r-s}\mathbb{Z}, \frac{\alpha\beta(p^{r-s}-1)x^2}{2p^{r-s}}\right) \\ &= \sqrt{p^s}\left(\frac{\alpha\beta}{p}\right)^{r-s}(-1)^{(r-s)(p^2-1)/8} \\ &= \left(\frac{\beta}{p}\right)^{r-s}\sqrt{p^s}\left(\frac{\alpha}{p}\right)^{r-s}(-1)^{(r-s)(p^2-1)/8}\end{aligned}$$

where the second to last equality follows from Theorem 2.4.1 and $\left(\cdot\right)$ is the Legendre symbol in the last two equalities. Notice that only β depends on our choice of quadratic form. Since $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{u}{p}\right) = -1$ the lemma is proven. □

In [7] certain invariants of symmetric bilinear forms are defined. We consider the multiplicative version of these invariants in the semigroup $\mu_8 \cup \{0\}$ considered under multiplication.

Definition 2.4.7. Let (G, b) be a non-degenerate discriminant form. Let $\tilde{G}_p^k = \frac{G[p^k]}{G[p^{k-1}]+pG[p^{k+1}]}$. Let $\tilde{b}_p^k : \tilde{G}_p^k \times \tilde{G}_p^k \to \mathbb{Q}/\mathbb{Z}$ be defined by

$$\tilde{b}_p^k([x],[y]) = p^{k-1}b(x,y) \tag{2.8}$$

for $x, y \in G[p^k]$.

Lemma 2.4.8. *Let (G, b) be a non-degenerate discriminant form where G has invariant factors $\{p_i^{r_i}\}_{i=1}^n$. Let k be a positive integer, and let p be a prime. Let N be the number of $i \in \{1, ..., n\}$ such that $p_i = p$ and $r_i = k$. The pair $(\tilde{G}_p^k, \tilde{b}_p^k)$ is a non-degenerate discriminant form where $\tilde{G}_p^k$ is a finite field of characteristic p and dimension N.*

Proof. Since $G \cong \bigoplus_{i=1}^n \mathbb{Z}/p_i^{r_i}\mathbb{Z}$, for each i let $e_i \in G$ be the element corresponding to $(0, ..., 1, ...0)$ where the 1 is in the i-th component. Then for any $g \in G$ there exists unique integers $a_i \in \{0, ..., p_i^{r_i} - 1\}$ such that $g = \sum_{i=1}^n a_i e_i$. Now $p^k g = 0$ if and only if $p^k a_i e_i = 0$ for all i if and only if $v_{p_i}(p^k a_i) \geq r_i$. If $p_i \neq p$, then $p^k g = 0$ implies $a_i = 0$. If $p_i = p$, then $p^k g = 0$ implies $v_p(a_i) \geq r_i - k$. This tells us $p^k g = 0$ implies

$$g = \sum_{i\,:\,p_i=p} p^{\min\{r_i-k,0\}} b_i e_i$$

where b_i is the integer such that $p^{\min\{r_i-k,0\}} b_i = a_i$. Thus

$$G[p^k] \cong \bigoplus_{i\,:\,p_i=p} \mathbb{Z}/p^{\min\{r_i,k\}}\mathbb{Z} \cong \bigoplus_{i\,:\,p_i=p} \left\langle p^{\min\{r_i-k,0\}} e_i \right\rangle.$$

By definition, $G[p^{k-1}]$ and $pG[p^{k+1}]$ are subgroups of $G[p^k]$. Let $i \in \{1, ..., n\}$ such that $p_i = p$. If $r_i < k$, then $e_i \in G[2^{k-1}]$. If $r_i > k$, then $p^{r_i-k} e_i \in pG[2^{k+1}]$. However, if $r_i = k$, then $e_i \notin (G[p^{k-1}] + pG[p^{k+1}])$, and $ae_i \in (G[p^{k-1}] + pG[p^{k+1}])$ if and only if $p|a$. Thus

$$\tilde{G}_p^k \cong \bigoplus_{\substack{i\,:\,p_i=p \\ r_i=k}} \mathbb{Z}/p\mathbb{Z}$$

which is a finite field of characteristic p and dimension N. Let $g \in G[2^k]$ and let $i \in \{1, ..., n\}$ such that $p_i = p$. Then if $r_i < k$, $2^{k-1}b(g, e_i) = 0$. If $r_i > k$, $2^{k-1}b(g, p^{r_i-k}e_i) = 0$. If $r_i = k$, $p^{k-1}b(g, pe_i) = 0$. Thus $\tilde{b}_p^k$ is well defined. By definition, $\tilde{b}_p^k$ is bilinear. If $g \in G[2^k]$ such that the coset $[g] \in \tilde{G}_p^k$ is nonzero, then $p^{k-1}g \neq 0$, and so there exists an $h \in G[2^k]$ such that $b(p^{k-1}g, h) \neq 0$. This implies $\tilde{b}_p^k([g], [h]) \neq 0$. Thus $\tilde{b}_p^k$ is non-degenerate. This completes the lemma. □

Definition 2.4.9. Let (G, b) be a non-degenerate discriminant form. Define the characteristic element $c^k(b)$ be the unique element of $\tilde{G}_2^k$ specified by the identity

$$\tilde{b}_2^k(c^k(b), x) = \tilde{b}_2^k(x, x) \quad \text{for all } x \in \tilde{G}_2^k. \tag{2.9}$$

If $c^n(b) = 0$, let $q_n : G/G[2^n] \to \mathbb{Q}/\mathbb{Z}$ defined by $q_n([x]) = 2^{n-1}b(x, x)$.

Lemma 2.4.10. *Let (G, b) be a non-degenerate discriminant form, and let n be a positive number. If $c^n(b) = 0$, then $2^{n-1}b(x, x) = 0$ for all $x \in G[2^n]$.*

Proof. Let $x \in G[2^n]$. Then there exists $y \in \tilde{G}_2^n$ and $z \in (G[2^{n-1}] + 2G[2^{n+1}])$ such that $x = y + z$. Thus

$$2^{n-1}b(x, x) = 2^{n-1}b(y, y) + 2^n b(y, z) + 2^{n-1}b(z, z).$$

The last term of the right hand side is zero. This was shown in the proof of Lemma 2.4.8 while proving $\tilde{b}_2^n$ is well defined. The second term is zero since $y + z \in G[2^n]$. Thus

$$2^{n-1}b(x, x) = \tilde{b}_2^n(c^n(b), y) = 0.$$

□

Definition 2.4.11 ([7])**.** Let (G, b) be a non-degenerate discriminant form, and let n be a positive integer. If $c^n(b) \neq 0$, let $\sigma_n(b) = \infty$. Otherwise let $\sigma_n(b)$ be the element of $\mathbb{Z}/8\mathbb{Z}$ such that

$$\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right) = \Theta(G/G[2^n], 2^{n-1}b(x, x)) \tag{2.10}$$

A word ought to be said about a small difference between our definition and that found in [7]. In that paper the left hand side of equation (2.10) contained a real-valued scaler. We, however, have tools at our disposal to show that the right hand side of (2.10) has absolute value one. By Lemma 2.4.8, the pre-metric group $(G/G[2^n], 2^{n-1}b(x,x))$ is non-degenerate. Since Θ is multiplicative, it is only necessary to show for an irreducible non-degenerate (G,b). Lemma 2.4.4 and Lemma 2.4.5 show that the right-hand side of (2.10) is an eighth root of unity.

Theorem 2.4.12 ([7] Theorem 4.1)**.** *Two non-degenerate discriminant forms (G,b) and (G,b') for a 2-group G are isomorphic if and only if $\sigma_n(b) = \sigma_n(b')$ for all positive integers n.*

Lemma 2.4.13. *Let (G,b) be a non-degenerate discriminant form for G a 2-group, and let $n \geq 1$. Let q be a quadratic form such that $b_q = b$. Then*

$$\frac{1}{\sqrt{|G[2^n]|}}\Theta(G, 2^n q) = \mathbf{e}\left(\frac{\sigma_n(b)}{8}\right) \tag{2.11}$$

Proof. Since $2q(x) = b(x,x)$, the left hand side of equation (2.11) is equal to

$$\begin{aligned}
&\frac{1}{\sqrt{|G[2^n]| \cdot |G|}} \sum_{x \in G} \mathbf{e}\left(2^{n-1}b(x,x)\right) \\
=&\frac{1}{\sqrt{|G[2^n]| \cdot |G|}} \sum_{x \in G/G[2^n]} \sum_{y \in G[2^n]} \mathbf{e}\left(2^{n-1}b(x+y,x+y)\right) \\
=&\frac{1}{\sqrt{|G[2^n]| \cdot |G|}} \sum_{x \in G/G[2^n]} \mathbf{e}\left(2^{n-1}b(x,x)\right) \sum_{y \in G[2^n]} \mathbf{e}\left(2^{n-1}b(y,y)\right)
\end{aligned} \tag{2.12}$$

If $c^n(b) = 0$, then the inner sum of equation (2.12) is equal to $|G[2^n]|$ by Lemma 2.4.10, and the proof is complete by definition of $\sigma_n(b)$. However, if $c^n(b) \neq 0$ consider the inner sum from equation (2.12)

$$\begin{aligned}
\sum_{y \in G[2^n]} \mathbf{e}\left(2^{n-1}b(y,y)\right) &= \sum_{y \in \tilde{G}_2^n} \sum_{z \in (G[2^{n-1}]+2G[2^{n+1}])} \mathbf{e}\left(2^{n-1}b(y+z,y+z)\right) \\
&= \sum_{z \in (G[2^{n-1}]+2G[2^{n+1}])} \mathbf{e}\left(2^{n-1}b(z,z)\right) \sum_{y \in \tilde{G}_2^n} \mathbf{e}\left(\tilde{b}_2^n(c^n(b),y)\right)
\end{aligned}$$

Since $c^n(b) \neq 0$, the inner sum above is zero, which implies equation (2.12) is zero. Since we defined $\mathbf{e}(\infty) = 0$, the lemma holds. $\square$

Lemma 2.4.14. *Let (G,q) be an irreducible metric 2-group, i.e. $(G,q)=\left(\mathbb{Z}/2^r\mathbb{Z},\frac{\alpha x^2}{2^{r+1}}\right)$ for $\alpha\in\{1,-1\}$ if $r=1$, or $\alpha\in\{1,-1,5,-5\}$ if $r>1$ or $(G,q)=\left((\mathbb{Z}/2^r\mathbb{Z})^2,\frac{\alpha x_1^2+x_1x_2+x_2^2}{2^r}\right)$ for $\alpha\in\{0,1\}$. Let $\beta\in\{1,-1,5,-5\}$. Then the following are true:*

(i) $\Theta\left(G^2,\begin{pmatrix}2\gamma & 1\\ 1 & 2\gamma\end{pmatrix}\otimes q\right)=(-1)^{\mathrm{rank}(G)\gamma r}$ *for* $\gamma\in\{0,1\}$.

(ii) $\Theta(G,\beta 2^n q)=\sqrt{|G[2^n]|}(-1)^{\mathrm{rank}(G)\max\{r-n,0\}(\beta^2-1)/8}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}$.

Proof The proof of (i) will be broken into two cases. If $(G,q)=(\mathbb{Z}/2^r\mathbb{Z},2^{-r-1}\alpha x^2)$ for $\alpha\in\{1,-1,5,-5\}$, then Lemma 2.2.8 implies $\left(G^2,\begin{pmatrix}2\gamma & 1\\ 1 & 2\gamma\end{pmatrix}\otimes q\right)=((\mathbb{Z}/2^r\mathbb{Z})^2,2^{-r}(\gamma x_1^2+x_1x_2+\gamma x_2^2))$. Thus, the result follows from Lemma 2.4.5.

However, if $(G,q)=((\mathbb{Z}/2^r\mathbb{Z})^2,2^{-r}(\alpha x_1^2+x_1x_2+\alpha x_2^2))$ the gram matrix of the corresponding bilinear form $\left(G^2,\begin{pmatrix}2\gamma & 1\\ 1 & 2\gamma\end{pmatrix}\otimes b_q\right)$ is the left matrix below

$$\frac{1}{2^r}\begin{pmatrix}4\gamma\alpha & 2\gamma & 2\alpha & 1\\ 2\gamma & 4\gamma\alpha & 1 & 2\alpha\\ 2\alpha & 1 & 4\gamma\alpha & 2\gamma\\ 1 & 2\alpha & 2\gamma & 4\gamma\alpha\end{pmatrix}\xrightarrow{\mathrm{Flip}_{1,3}}\frac{1}{2^r}\begin{pmatrix}4\gamma\alpha & 1 & 2\alpha & 2\gamma\\ 1 & 4\gamma\alpha & 2\gamma & 2\alpha\\ 2\alpha & 2\gamma & 4\gamma\alpha & 1\\ 2\gamma & 2\alpha & 1 & 4\gamma\alpha\end{pmatrix}$$

Recall that row-column operations (Definition 2.2.2) yield a gram matrix associated to an isomorphic metric group. By Lemma 2.2.8 there exists a 2 by 2 integer matrix S such that

$$\frac{1}{2^r}(S\oplus S)^{\mathrm{tr}}\begin{pmatrix}4\gamma\alpha & 1 & 2\alpha & 2\gamma\\ 1 & 4\gamma\alpha & 2\gamma & 2\alpha\\ 2\alpha & 2\gamma & 4\gamma\alpha & 1\\ 2\gamma & 2\alpha & 1 & 4\gamma\alpha\end{pmatrix}(S\oplus S)\equiv\frac{1}{2^r}\begin{pmatrix}0 & 1 & x & y\\ 1 & 0 & z & w\\ x & z & 0 & 1\\ y & w & 1 & 0\end{pmatrix}\mod\mathbb{Z}$$

for some even integers x, y, z, and w. Since $G\oplus G$ is homogeneous, all row-column operations are valid. Then the following row-column operations yield

$$\frac{1}{2^r}\begin{pmatrix}0 & 1 & x & y\\ 1 & 0 & z & w\\ x & z & 0 & 1\\ y & w & 1 & 0\end{pmatrix}\xrightarrow{\mathrm{Add}_3^{-z,1},\mathrm{Add}_3^{-x,2},\mathrm{Add}_4^{-w,1},\mathrm{Add}_4^{-y,2}}\frac{1}{2^r}\begin{pmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & -2xz & 1-wx-yz\\ 0 & 0 & 1-wx-yz & -2wy\end{pmatrix}$$

Since x, y, z, and w are even, Lemma 2.2.8 implies there exists a 2 by 2 integer matrix S' such

that

$$\frac{1}{2^r}(I_2 \oplus S')^{\mathrm{tr}} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2xz & 1-wx-yz \\ 0 & 0 & 1-wx-yz & -2wy \end{pmatrix} (I_2 \oplus S') \equiv \frac{1}{2^r} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \mod \mathbb{Z}$$

Thus $\left(G^2, \begin{pmatrix} 2\gamma & 1 \\ 1 & 2\gamma \end{pmatrix} \otimes q\right) \cong ((\mathbb{Z}/2^r\mathbb{Z})^2, (x_1x_2)/2^r) \oplus ((\mathbb{Z}/2^r\mathbb{Z})^2, (x_1x_2)/2^r)$. The result follows from Lemma 2.4.5.

The proof of (ii) will be broken into several cases.

Case 1: If $n > r$, then $\Theta(G, \beta 2^n q) = \sqrt{|G[2^n]|}$, and $(-1)^{\mathrm{rank}(G)\max\{r-n,0\}(\beta^2-1)/8} = 1$. Also, $\tilde{G}_2^n$ is the zero group, which means $c^n(b) = 0$, and the Gauss sum $\mathbf{e}(0) = 1 = \mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)$. Thus the equation holds.

Case 2: If $n = r$ and $\mathrm{rank}(G) = 1$, then

$$\Theta(G, \beta 2^n q) = \sum_{x=0}^{2^{r-1}-1} \sum_{y=0}^{1} \mathbf{e}\left(\frac{\beta\alpha(2x+y)^2}{2}\right) = \sum_{x=0}^{2^{r-1}-1} \sum_{y=0}^{1} (-1)^y = 0$$

which shows the left hand side of (ii) is zero. Also, if $\beta = 1$ Lemma 2.4.13 implies $\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right) = 0$. Thus the equation holds.

Case 3: If $n < r$ and $\mathrm{rank}(G) = 1$, then notice that

$$\begin{aligned} (\alpha^2\beta^2 - 1)/8 &\equiv (\alpha^2 - 1)/8 + (\beta^2 - 1)/8 \mod 2 \\ &\equiv ((\alpha^2 - 1)/8)^\beta + (\beta^2 - 1)/8 \mod 2. \end{aligned}$$

Thus

$$\begin{aligned}
\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, \frac{\beta\alpha x^2}{2^{r-n+1}}\right) &= \frac{1}{\sqrt{2^r}} \sum_{x=0}^{2^r-1} \mathbf{e}\left(\frac{\beta\alpha x^2}{2^{r-n+1}}\right) \\
&= \frac{1}{\sqrt{2^r}} \sum_{x=0}^{2^{r-n}-1} \sum_{y=0}^{2^n-1} \mathbf{e}\left(\frac{\beta\alpha(x+2^{r-n}y)^2}{2^{r-n+1}}\right) \\
&= \frac{\sqrt{2^n}}{\sqrt{2^{r-n}}} \sum_{x=0}^{2^{r-n}} \mathbf{e}\left(\frac{\beta\alpha x^2}{2^{r-n+1}}\right) \\
&= \sqrt{2^n}(-1)^{(r-n)(\alpha^2\beta^2-1)/8}\mathbf{e}\left(\frac{\beta\alpha}{8}\right) \\
&= \sqrt{2^n}(-1)^{(r-n)(\beta^2-1)/8}\left((-1)^{(r-n)(\alpha^2-1)/8}\mathbf{e}\left(\frac{\alpha}{8}\right)\right)^{\beta} \\
&= \sqrt{|G[2^n]|}(-1)^{\operatorname{rank}(G)\max\{r-n,0\}(\beta^2-1)/8}\left(\frac{\Theta\left(\mathbb{Z}/2^r\mathbb{Z}, 2^n\frac{\alpha x^2}{2^{r+1}}\right)}{\sqrt{G[2^n]}}\right)^{\beta} \\
&= \sqrt{|G[2^n]|}(-1)^{\operatorname{rank}(G)\max\{r-n,0\}(\beta^2-1)/8}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}.
\end{aligned}$$

Thus the equation holds.

Case 4: If $\operatorname{rank}(G) = 2$ and $n \leq r$, then since $\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right) \in \{1, -1\}$

$$(-1)^{\operatorname{rank}(G)\max\{r-n,0\}(\beta^2-1)/8}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta} = \mathbf{e}\left(\frac{\sigma_n(b)}{8}\right).$$

Also, by Lemma 2.2.8 we know that

$$\Theta\left((\mathbb{Z}/2^r\mathbb{Z})^2, \beta\frac{\alpha x_1^2 + x_1x_2 + \alpha x_2^2}{2^{r-k}}\right) = \Theta\left((\mathbb{Z}/2^r\mathbb{Z})^2, \frac{\alpha x_1^2 + x_1x_2 + \alpha x_2^2}{2^{r-k}}\right)$$

for all $k \leq r$. Thus the left hand side of (ii) is equal to $\Theta(G, 2^n q)$, which, by Lemma 2.4.13 is equal to $\sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)$. This completes the proof. □

CHAPTER 3. DETERMINING THE FROBENIUS SCHUR INDICATOR OF TAMBARA YAMAGAMI CATEGORIES

3.1 The Frobenius-Schur Indicator of Tambara Yamagami Categories

Definition 3.1.1 ([17] p. 550)**.** Let (G, b) be a discriminant form. Let $\tau = \pm|G|^{-1/2}$. A *Tambara-Yamagami category* $\mathcal{C} = \mathcal{TY}(G, b, \tau)$ is the category with objects finite direct sums of elements of $S := G \cup \{m\}$ satisfying the fusion rules

$$g \otimes h = (g + h) \qquad g \otimes m = m = m \otimes g \qquad m \otimes m = \bigoplus_{x \in G} x \quad (g, h \in G)$$

with the unit object being 0_G. The left and right unit constraints are identity morphisms. Hom-sets between elements of S are given by

$$\mathrm{Hom}(s, s') = \begin{cases} \mathbb{C} & \text{if } s = s' \\ 0 & \text{otherwise} \end{cases}$$

and the composition of morphisms are obvious ones. The associativity constraint Φ is determined by

$$\Phi_{g,m,h} = \mathbf{e}(-b(g,h))\,\mathrm{id}_m : m \to m,$$
$$\Phi_{m,g,m} = \left(\mathbf{e}(-b(g,x))\delta_{x,y}\,\mathrm{id}_x\right)_{x,y} : \bigoplus_{x \in G} x \to \bigoplus_{y \in G} y,$$
$$\Phi_{m,m,m} = \left(\tau\mathbf{e}(b(x,y))\,\mathrm{id}_m\right)_{x,y} : \bigoplus_{x \in G} m \to \bigoplus_{y \in G} m,$$

where $g, h \in G$ and the other $\Phi_{s,t,u}$, $(s, t, u \in S)$ are identity morphisms.

Definition 3.1.2. Let (G, b) be a non-degenerate discriminant form. Let $C(b)$ be the set of functions $\varphi : G \to \mathbb{Q}/\mathbb{Z}$ such that $b(x, y) = \varphi(x + y) - \varphi(x) - \varphi(y)$.

Remark 3.1.3. Notice that $C(b)$ is non-empty since there exists a quadratic form q such that $b_q = b$. One may also check that the map $a \mapsto \varphi_a$ where

$$\varphi_a(x) = q(x) + b(x, a)$$

is a bijection between G and $C(b)$.

Lemma 3.1.4 (Shimizu)**.** *Let (G, b) be a discriminant form and let $\varphi \in C(b)$. Then $\varphi|_{\mathrm{Rad}(b)}$ is a character of* $\mathrm{Rad}(b)$ *and*

$$\frac{1}{\mathrm{Rad}(b)|} \sum_{x \in Rad(b)} \mathbf{e}(\varphi(x)) = \begin{cases} 1 & \text{if } \varphi \text{ is trivial on } \mathrm{Rad}(b). \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Proof. If $g \in G$ and $x \in \mathrm{Rad}(b)$ then

$$\varphi(g) + \varphi(x) = \varphi(g + x) + b(g, x) = \varphi(g + x) \tag{3.2}$$

Thus $\mathbf{e} \circ \varphi|_{\mathrm{Rad}(b)}$ is a character of $\mathrm{Rad}(b)$ and 3.1 is true by the orthogonality of characters. □

3.2 Building the Discriminant Form

In this section we shall relate the Frobenius-Schur indicator of the element m of the category $\mathcal{TY}(G, b, \tau)$ with certain Gauss sums for some pre-metric groups defined in terms of (G, b).

Definition 3.2.1. Let (G, q) be a pre-metric group, and let k be a positive integer. Let $\mathcal{F}_k(G) = \left\{(a_1, ..., a_k) \in G^k \;\middle|\; \sum_{i=1}^k a_i = 0\right\}$ and let $\mathcal{F}_k(q) : \mathcal{F}_k(G) \to \mathbb{Q}/\mathbb{Z}$ be defined by

$$\mathcal{F}_k(q)(a_1, ..., a_k) = \sum_{i=1}^{k} q(a_i).$$

For a morphism of pre-metric groups $f : (G, q) \to (H, u)$ let $\mathcal{F}_k(f) : \mathcal{F}_k(G, q) \to \mathcal{F}_k(H, u)$ be defined by

$$\mathcal{F}_k(f)(g_1, ..., g_k) = (f(g_1), ..., f(g_k)).$$

Lemma 3.2.2. *Let k be a positive integer.*

- *The symbol $\mathcal{F}_k$ defines an endofunctor on the category* **Quad** *of pre-metric groups.*

- *If* $(G,q) = (H,u) \perp (L,w)$ *then* $\mathcal{F}_k(G,q) = \mathcal{F}_k(H,u) \perp \mathcal{F}_k(L,w)$.

Proof. The proof of the first item is seen by checking that $\mathcal{F}_k(G,q)$ is a pre-metric group and $\mathcal{F}_k(f)$ preserves the quadratic form.

Since $G^k = H^k \oplus L^k$ we have

$$\mathcal{F}_k(G) = \left\{ (g_1, ...g_k) \in G^k : \sum_{i=1}^k g_i = 0 \right\} = \left\{ (h_1, ..., h_k, l_1, ...l_k) \in H^k \oplus L^k : \sum_{i=1}^k h_i + \sum_{j=1}^k l_j = 0 \right\}$$

But since $H \cap L = 0$,

$$\sum_{i=1}^k h_i = -\sum_{j=1}^k l_j \quad \Longrightarrow \quad \sum_{i=1}^k h_i = 0 = \sum_{j=1}^k l_j$$

Thus

$$\mathcal{F}_k(G) = \mathcal{F}_k(H) \oplus \mathcal{F}_k(L)$$

Let $(g_1, ..., g_k) = (h_1 + l_1, ..., h_k + l_k) \in \mathcal{F}_k(G) = \mathcal{F}_k(H) \oplus \mathcal{F}_k(L)$. Then

$$F_k(q)(g_1, ..., g_k) = \sum_{i=1}^k q(g_i) = \sum_{i=1}^k (u(h_i) + w(l_i)) = F_k(u)(h_1, ..., h_k) + F_k(w)(l_1, ..., l_k).$$

This proves the lemma. □

Lemma 3.2.3. *Let* (G,b) *be a non-degenerate discriminant form. Let* q *be a quadratic form such that* $b_q = b$. *Then* $\mathrm{Rad}(\mathcal{F}_k(q)) \cong G[k]$.

Proof. Let $J_k = \{(a, a, ..., a) \in \mathcal{G}_k \mid k \cdot a = 0\}$. Let $\overline{g} = (g_1, \cdots, g_k) \in \mathrm{Rad}(\mathcal{F}_k(G,b))$ Then $0 = \sum b(g_i, h_i)$ for all $(h_1, \cdots, h_k) \in \mathcal{F}_k(G)$. Let $h \in G$. Since $(h, -h, 0, \cdots, 0) \in \mathcal{F}_k(G)$ we have $0 = b(g_1, h) + b(g_2, -h) = b(g_1 - g_2, h)$ for all $h \in G$. Since b is non-degenerate, this implies $g_1 = g_2$. Similarly, we get $g_2 = g_3$ etcetera. So $\overline{g} = (g_1, g_1, \cdots, g_1)$. Since $\overline{g} \in \mathcal{F}_k(G)$, we have $kg_1 = 0$. So $\overline{g} \in J_k$. The inclusion is clear. Recalling our definition of $G[k] = \{a \in G | k \cdot a = 0\}$ we see that $J_k \cong G[k]$. □

The following theorem combines Theorem 3.2 and 3.4 from [17] with one small change: we express the indicator of m as a Gauss sum.

Theorem 3.2.4. *Let* (G,b) *be a non-degenerate discriminant form. Let* $\tau = \pm|G|^{-1/2}$. *Let* $\mathcal{C}$ *be the Tambara-Yamagami category* $\mathcal{TY}(G,b,\tau)$. *Let* q *be a quadratic form such that* $b_q = b$.

Let k be a positive integer. Then for any $g \in G$, $\nu_k(g) = \delta_{1,kg}$ where δ is the Kronecker delta symbol, $\nu_{2k-1}(m) = 0$, and

$$\nu_{2k}(m) = \mathrm{sgn}(\tau)^k \Theta(\mathcal{F}_k(G, q)) \tag{3.3}$$

Proof: From the definition of Tambara-Yamagami categories it follows that if $kg \neq 0$ then $\mathrm{Hom}(kg, 0)$ is the 0 vector space and so that case is proven trivially. However, if $kg = 0$, then $\mathrm{Hom}\, kg, 0 = \mathbb{C}$. Consider the automorphism $E_g^n : \mathrm{Hom}(kg, 0) \to \mathrm{Hom}(kg, 0)$ as defined in Definition 1.4.10. By definition, the morphisms j_g, ev_g, coev_g, and $\Phi_{a,b,c}$ for $a, b, c \in G$ are all identity morphisms, which implies $E_g^n(f) = f$ for all $f \in \mathrm{Hom}(kg, 0)$. Thus, in this case $\nu_k(g) = \mathrm{Tr}(\mathrm{id}) = 1$.

Recall the bijection between G and $C(b)$ in Remark 3.1.3 defined by $a \mapsto \varphi_a$ where $\varphi_a(x) = q(x) + b(x, a)$. In [17] the simple objects of the double of the Tambara-Yamagami category are given. The simple objects (X, e_X) such that $\mathrm{Hom}_{\mathcal{C}}(X, m)$ is non-zero are pairs $(m, u_{\varphi,\Delta})$ where $\varphi \in C(b)$ and where

$$\Delta = \pm\sqrt{\tau \sum_{x \in G} \mathbf{e}(\varphi(x))}$$

It is also shown that

$$\theta_{(m,u_{\varphi,\Delta})} = \Delta$$

Using the equation from Theorem 1.4.11

$$\begin{aligned}
\nu_{2k}(m) &= \frac{1}{\operatorname{pdim}\mathcal{C}} \sum_{(X,e_x)\in\Gamma} \theta_X^{2k} \operatorname{pdim}(X) \dim_{\mathbb{C}}(\operatorname{Hom}(m,X)) \\
&= \frac{1}{2|G|} \sum_{\substack{\varphi\in C(b) \\ \epsilon\in\{1,-1\}}} \left(\epsilon\sqrt{\tau\sum_{x\in G}\mathbf{e}(\varphi(x))}\right)^{2k} \left(\sqrt{|G|}\right) (1) \\
&= \frac{1}{\sqrt{|G|}} \sum_{y\in G} \left(\frac{\operatorname{sgn}(\tau)}{\sqrt{|G|}} \sum_{x\in G}\mathbf{e}(\varphi_y(x))\right)^k \qquad (3.4) \\
&= \frac{\operatorname{sgn}(\tau)^k}{|G|^{(k+1)/2}} \sum_{x_1,\dots,x_k\in G} \mathbf{e}(q(x_1))\dots\mathbf{e}(q(x_k)) \sum_{y\in G}\mathbf{e}(b(x_1+\dots+x_k,y)) \\
&= \frac{\operatorname{sgn}(\tau)^k}{|G|^{(k-1)/2}} \sum_{x_1+\dots+x_k=0} \mathbf{e}(q(x_1))\dots\mathbf{e}(q(x_k)) \\
&= \frac{\operatorname{sgn}(\tau)^k}{\sqrt{|\mathcal{F}_k(G)|}} \sum_{a\in\mathcal{F}_k(G)} e(\mathcal{F}_k(q)(a))
\end{aligned}$$

By definition of $\Theta(\mathcal{F}_k(G,q))$ the theorem is proven. □

By summing over cosets of $J_k = \operatorname{Rad}(\mathcal{F}_k(q))$ the above equation is equivalent to

$$\nu_{2k}(m) = \frac{\operatorname{sgn}(\tau)^k}{\sqrt{|G[k]|}} \cdot \frac{1}{\sqrt{|\mathcal{F}_k(G)/J_k|}} \sum_{a+J_k\in\mathcal{F}_k(G)/J_k} \mathbf{e}(\mathcal{F}_k(q)(a)) \sum_{r\in J_k}\mathbf{e}(\mathcal{F}_k(q)(r)) \qquad (3.5)$$

Theorem 3.2.5 ([17] Theorem 3.5)**.** *Let (G,b) be a non-degenerate discriminant form. Let $\tau = \pm|G|^{-1/2}$. Let $\mathcal{C}$ be the Tambara-Yamagami $\mathcal{TY}(G,b,\tau)$. Let q be a quadratic form such that $b_q = b$. Let k be a positive integer. Then $\nu_{2k}(m) = \sqrt{|G[k]|}\cdot\xi$ for some $\xi\in\mu_8\cup\{0\}$ where $\xi = 0$ if and only if there exists $a\in G[k]$ such that $kq(a)\neq 0$.*

Let $J_k = \operatorname{Rad}(\mathcal{F}_k(q))$.

Case 1: If there exists $a\in G[k]$ such that $kq(a)\neq 0$, then $\mathbf{e}\circ\mathcal{F}_k(q)$ is nontrivial on J_k. By Lemma 3.1.4, $\mathbf{e}\circ\mathcal{F}_k(q)$ is a nontrivial character on J_k, so equation (3.5) is equal to zero, which gives us

$$\nu_{2k}(m) = 0$$

Case 2: If $kq(a) = 0$ for all $a\in G[k]$, then $\mathbf{e}\circ\mathcal{F}_k(q)$ is trivial on J_k. In this case $\mathcal{F}_k(q)$ induces a non-degenerate form (denoted by the same symbol) on $\mathcal{F}_k(G)/J_k$. Again using

Lemma 3.1.4 we have

$$\nu_{2k}(m) = \mathrm{sgn}(\tau)^k \sqrt{|G[k]|} \left(\frac{1}{\sqrt{|\mathcal{F}_k(G)/J_k|}} \sum_{a \in \mathcal{F}_k(G)/J_k} \mathbf{e}\left(\mathcal{F}_k(q)(a)\right) \right) \tag{3.6}$$

The part inside the parentheses is an 8th root of unity by Milgram's formula, which can be found in Appendix 4 of [10].

If (L, B) is some integer lattice such that L'/L is G_k/J_k, then this 8th root of unity is just $\mathbf{e}(\text{signature}(L))$.

$$\nu_{2k}(m) = \mathrm{sgn}(\tau)^k \sqrt{|G[k]|} \cdot \mathbf{e}\left(\frac{\xi}{8}\right)$$

where ξ is the signature of L.

Remark 3.2.6. The case when $k = 1$ can be computed directly. By Theorem 3.2.4

$$\nu_2(m) = \mathrm{sgn}(\tau)\Theta(\mathcal{F}_1(G, q)) = \mathrm{sgn}(\tau)\Theta(G[1], q) = \mathrm{sgn}(\tau).$$

Remark 3.2.7. Assume the setup of Theorem 3.2.4. Suppose order of G is odd. Let $|G| = n$. Then the exponent of $G[k]$ is a factor of $k_1 = k/2^{v_2(k)}$. As we saw in Lemma 2.1.9, the quadratic form q restricted to $G[k]$ then takes values in $k_1^{-1}\mathbb{Z}/\mathbb{Z}$. So for all $a \in G[k]$, we have $k_1 q(a) = 0$, a fortiori $kq(a) = 0$. So if G has odd order then $\nu_{2k}(m)$ is always non-zero.

On the other hand, consider the quadratic form on $\mathbb{Z}/2^r\mathbb{Z}$ given by $q(x) = \alpha x^2/2^{r+1}$ with $\alpha \in \{\pm 1, \pm 5\}$. Let a be a generator of $\mathbb{Z}/2^r\mathbb{Z}$. Let k be an positive integer such that $v_2(k) = r$. Then $ka = 0$ but $kq(a) \neq 0$, so $\Theta(\mathcal{F}_{2k}(G, q)) = \nu_{2k}(m) = 0$. Decomposing (G, q) into irreducible components and using the multiplicativity of Θ we conclude that if an irreducible decomposition of (G, b) contains a form of type $A_{2^r}, B_{2^r}, C_{2^r}$ or D_{2^r} then $\nu_{2k}(m) = 0$ for all k with $v_2(k) = r$.

3.3 The Indicator as a Gauss Sum

Definition 3.3.1. Let G be a finite abelian group and k be a positive integer. Then let $\phi_{G,k} : G^{k-1} \to \mathcal{F}_k(G)$ be defined by

$$\phi(g_1, ..., g_{k-1}) = \left(g_1, ..., g_{k-1}, \sum_{i=1}^{k-1} -g_i \right)$$

Lemma 3.3.2. *Let (G,q) be a metric group and let k be a positive integer. Let T_k be the $(k-1)\times(k-1)$ matrix with two's on the diagonal and one's on the off-diagonal entries. Then $\phi_{G,k}:(G^{k-1},T_k\otimes q)\to\mathcal{F}_k(G,q)$ is a pre-metric group isomorphism.*

Proof. One verifies that this is a group isomorphism. What is left to show is that $\mathcal{F}_k(q)\circ\phi_{G,k}=T_k\otimes q$. Let $(g_1,...,g_{k-1})\in G^{k-1}$. Then

$$\begin{aligned}\mathcal{F}_k(q)\circ\phi_{G,k}(g_1,...,g_{k-1}) &= \mathcal{F}_k(q)\left(g_1,...,g_{k-1},\sum_{i=1}^{k-1}-g_i\right)\\ &=\sum_{i=1}^{k-1}q(g_i)+\sum_{i=1}^{k-1}q(g_i)+\sum_{1\le i<j\le k}b(g_i,g_j)\\ &=T_k\otimes q(g_1,...,g_{k-1})\end{aligned}$$

where the second equality follows from the fact that $q(x)=q(-x)$ and Lemma 2.1.9. □

Remark 3.3.3. Let (G,b) be a discriminant form, and let q_1 and q_2 be quadratic forms on G such that $b_{q_1}=b=b_{q_2}$. Then for any positive k, $(G^{k-1},T_k\otimes q_1)\cong(G^{k-1},T_k\otimes q_1)$.

Proof. By our assumption, $2q_1(x)=b(x,x)=2q_2(x)$. Then

$$T_k\otimes q_1(x_1,...,x_{k-1})=\sum_{i=1}^{k-1}b(x_i,x_i)+\sum_{1\le i<j\le k-1}b(x_i,x_j)=T_k\otimes q_2(x_1,...,x_{k-1}).$$

□

Theorem 3.3.4. *Let $G=\mathbb{Z}/p^r\mathbb{Z}$ for some odd prime p and positive integer r. Let k be a positive integer and let u be a quadratic non-residue of $\mathbb{Z}/p\mathbb{Z}$. Then there exist integers $d_1,...,d_{k-1}$ with $d_i\in\{1,u\}$ for all $i\in[k-1]$ such that for any non-degenerate quadratic form q on G*

$$\Theta\left(\mathcal{F}_k(G,q)\right)=\Theta\left(G,d_{k-1}p^{\min\{r,v_p(k)\}}\cdot q\right)\prod_{i=1}^{k-2}\Theta(G,d_i\cdot q).$$

Proof. By Theorem 2.2.10 we may assume $q(x)=2^{-1}\alpha x^2/p^r$ for $\alpha\in\{1,u\}$ and $2^{-1}=(p^r+1)/2$. By Lemma 3.3.2 $\mathcal{F}_k(G,q)\cong(G^{k-1},T_k\otimes q)$. Consider $p^{-r}T_k$ as a symmetric matrix with entries in $p^{-r}\mathbb{Z}/\mathbb{Z}$. By Lemma 2.2.5 there exists some $S\in M_{k-1}(\mathbb{Z})$ such that S mod $p\in GL_{k-1}(\mathbb{Z}/p\mathbb{Z})$ and

$$S^T\left(p^{-r}T_k\right)S=\operatorname{diag}(d_1p^{-s_1},...,d_{k-1}p^{-s_{k-1}})\quad\text{in}\quad M_n(p^{-r}\mathbb{Z}/\mathbb{Z}).$$

where $d_i \in \{1, u\}$ for all $i \in [k-1]$ and $r \geq s_1 \geq ... \geq s_{k-1} \geq 0$. Thus

$$D = \text{diag}(d_1 p^{r-s_1}, ..., d_{k-1} p^{r-s_{k-1}})$$

has integer entries. Since G^{k-1} is homogeneous, all row-column operations on the gram matrix are valid. Since $S^T T_k S \equiv D \mod p^r$, Lemma 2.3.5 implies

$$(G^{k-1}, T_k \otimes q) \cong (G^{k-1}, S^T T_k S \otimes q) \cong (G^{k-1}, D \otimes q). \tag{3.7}$$

Since q is non-degenerate,

$$\text{Rad}(D \otimes q) \cong \bigoplus_{i=1}^{k-1} \mathbb{Z}/p^{r-s_i}\mathbb{Z} \tag{3.8}$$

However, Lemma 3.2.3 implies $\text{Rad}(D \otimes q) \cong G[k]$. Now $G[k]$ is cyclic p-group, as it is a subgroup of a cyclic p-group. This means all but one of the diagonal entries of D are relatively prime to p. Since $s_1 \leq ... \leq s_{k-1}$ this implies $s_i = r$ for all $i \in [k-2]$, but $r - s_{k-1} = v_p(|G[k]|)$. Now $v_p(|G[k]|) = v_p(|G[p^{v_p(k)}]|) = \min(r, v_p(k))$. By definition of the orthogonal sum

$$\mathcal{F}_k(G, q) \cong (G, d_1 \cdot q) \perp ... \perp (G, d_{k-2} \cdot q) \perp (G, d_{k-1} p^{\min\{r, v_p(k)\}} \cdot q).$$

Thus, by the multiplicative nature of Θ, the lemma is proven. □

Lemma 3.3.5. *Let p be an odd prime and r and k be positive integers. Let u be a quadratic non-residue of $\mathbb{Z}/p\mathbb{Z}$. Let $(G, q_1) = (\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2))$ and $(G, q_2) = (\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2))$. Then*

$$\Theta\left(\mathcal{F}_k(G, q_1)\right) = (-1)^{r(k-1)-\min\{r, v_p(k)\}} \Theta\left(\mathcal{F}_k(G, q_2)\right).$$

Proof. By Theorem 3.3.4

$$\Theta\left(\mathcal{F}_k(G, q_1)\right) = \Theta\left(G, d_{k-1} p^{\min\{r, v_p(k)\}} \cdot q_1\right) \prod_{i=1}^{k-2} \Theta(G, d_i \cdot q_1),$$

$$\Theta\left(\mathcal{F}_k(G, q_2)\right) = \Theta\left(G, d_{k-1} p^{\min\{r, v_p(k)\}} \cdot q_2\right) \prod_{i=1}^{k-2} \Theta(G, d_i \cdot q_2).$$

By Lemma 2.4.6

$$\Theta\left(\mathcal{F}_k(G, q_1)\right) = (-1)^{r(k-1)-\min\{r, v_p(k)\}} \Theta\left(\mathcal{F}_k(G, q_2)\right).$$

This proves the lemma. □

Lemma 3.3.6. *Let (G,b) and (G,b') be non-degenerate discriminant forms for an odd-order group G. Let q and q' be a quadratic forms such that $b_q = b$ and $b_{q'} = b'$ respectively. If $(G,b) \ncong (G,b')$ then their exists an integer k such that*

$$\Theta(\mathcal{F}_k(G,q)) \neq \Theta(\mathcal{F}_k(G,q'))$$

and k is either odd, or k has arbitrary positive 2-valuation.

Proof. Since the Gauss sums are invariants of discriminant forms, if the Gauss sums are not equal, then the discriminant forms are not isomorphic. For the other direction we will prove the contrapositive. By the Structure Theorem of finite abelian groups $G \cong \bigoplus_{i=1}^{n} N_i\,(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$ where for each $i \in \{1,...,n\}$, p_i is an odd prime, r_i and N_i are a positive integers, and pairs (p_i,r_i) are unique. Note that primes p_i may be repeated. By Theorem 2.2.10 (G,q) is isomorphic to a orthogonal direct sum of metric groups $(H_i,q_i) = (\mathbb{Z}/p_i^{r_i}\mathbb{Z}, p^{-r}(2^{-1}\alpha_i x^2))$ and (G,q') is isomorphic to a orthogonal direct sum of metric groups $(H_i,q_i) = (\mathbb{Z}/p_i^{r_i}\mathbb{Z}, p^{-r}(2^{-1}\alpha_i' x^2))$ where for each $i \in \{1,...,n\}$ u_i is a quadratic non-residue of $\mathbb{Z}/p_i\mathbb{Z}$ and α_i, $\alpha_i' \in \{1,u_i\}$.. Let $N_{p,r} = |\{(p_i,r_i) : (p_i,r_i) = (p,r)\}|$. By Lemma 2.2.11,

$$\Theta(G,q) = \prod_{p,r:N_{p,r}>0} \Theta(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2))^{N_{p,r}-1}\Theta(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}\alpha_{p,r}x^2))$$

$$\Theta(G,q') = \prod_{p,r:N_{p,r}>0} \Theta(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2))^{N_{p,r}-1}\Theta(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}\alpha'_{p,r}x^2))$$

Let

$$\mathcal{A} = \{(p,r) : N_{p,r} > 0 \text{ and } \alpha_{p,r} \neq \alpha'_{p,r}\} \quad \text{and} \quad \mathcal{A}_{\max} = \{(p,r) \in \mathcal{A} : (p,r') \notin \mathcal{A} \text{ for all } r' > r\}.$$

Let

$$\Lambda = \sum_{(p,r)\in\mathcal{A}} (r(k-1) - \min\{r, v_p(k)\}) \mod 2.$$

Then

$$\begin{aligned}
\Theta\big(\mathcal{F}_k(G,q)\big) &= \prod_{(p,r)\,:\,N_{p,r}>0} \Theta(\mathcal{F}_k(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2)))^{N_{p,r}-1}\Theta(\mathcal{F}_k(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}\alpha_{p,r}x^2))) \\
&= (-1)^{\Lambda} \prod_{(p,r)\,:\,N_{p,r}>0} \Theta(\mathcal{F}_k(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}x^2)))^{N_{p,r}-1}\Theta(\mathcal{F}_k(\mathbb{Z}/p^r\mathbb{Z}, p^{-r}(2^{-1}\alpha'_{p,r}x^2))) \\
&= (-1)^{\Lambda}\Theta\big(\mathcal{F}_k(G,q')\big)
\end{aligned}$$

Case 1: If there exists a prime p such that $(p,1) \in \mathcal{A}_{\max}$ let $k = p$. We see that

$$(1)(k-1) - \min\{1, v_p(k)\} = p - 2 \equiv 1 \mod 2$$

and for all $(p', r) \in \mathcal{A}$ such that $p' \neq p$

$$r(k-1) - \min\{r, v_{p'}(k)\} = r(p-1) \equiv 0 \mod 2.$$

Thus $\Lambda \equiv 1 \mod 2$, and so k is odd and $\Theta(\mathcal{F}_k(G,q)) \neq \Theta(\mathcal{F}_k(G,q'))$.

Case 2: Otherwise, there exists a $(p,r) \in \mathcal{A}_{\max}$ such that $r > 1$. Let

$$k = \frac{2^\gamma}{p} \prod_{(p',r') \in \mathcal{A}_{\max}} (p')^{r'}.$$

Then

$$r(k-1) - \min\{r, v_p(k)\} \equiv r - (r-1) = 1 \mod 2.$$

For any $r' < r$ such that $(p,r) \in \mathcal{A}$ we have

$$r'(k-1) - \min\{r', v_p(k)\} \equiv r' - r' = 0 \mod 2.$$

For any $(p', r') \in \mathcal{A}$ such that $p' \neq p$ we have

$$r'(k-1) - \min\{r', v_{p'}(k)\} \equiv r' - r' = 0 \mod 2.$$

Thus $\Lambda \equiv 1 \mod 2$, and so $v'(k) = \gamma$ and $\Theta(\mathcal{F}_k(G,q)) \neq \Theta(\mathcal{F}_k(G,q'))$. This completes the theorem. □

Lemma 3.3.7. *Let r and k be positive integers. Consider the matrix T_k from Lemma 3.3.2. Then there exists a $S \in M_{k-1}(\mathbb{Z}/2^r\mathbb{Z})$ such that*

$$S^{\mathrm{tr}} T_k S \cong \begin{cases} \left(\bigoplus_{i=1}^{\lfloor \frac{k+1}{4} \rfloor} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right) \oplus \left(\bigoplus_{j=1}^{\lfloor \frac{k-1}{4} \rfloor} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) \oplus [\beta 2^{v_2(k)}] & \text{if } k \text{ is even} \\ \left(\bigoplus_{i=1}^{\lfloor \frac{k+1}{4} \rfloor} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right) \oplus \left(\bigoplus_{j=1}^{\lfloor \frac{k-1}{4} \rfloor} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) & \text{if } k \text{ is odd.} \end{cases}$$

in $M_{k-1}(\mathbb{Z}/2^r\mathbb{Z})$ for $\beta \in \{1, -1, 5, -5\}$.

Proof. Let $H_{k-1} \in M_{k-1}(\mathbb{Z})$ be the matrix such that every entry is equal to 1. Let $I_{k-1} \in M_{k-1}(\mathbb{Z})$ be the identity matrix. Let $T_{k,a} = I_{k-1} + aH_{k-1}$ for some integer a. Notice that $T_{k,1} = T_k$. The proof works inductively by showing that for every odd integer a and $k \geq 4$, there exists a matrix $S \in M_{k-1}(\mathbb{Z})$ such that $S^{\text{tr}} T_{k,a} S \equiv A \oplus T_{k-2,c} \mod 2^r$ for c an odd integer. Let z be an integer such that $z(2a+1) \equiv 1 \mod 2^r$. For each i such that $2 < i < k$ we perform the row-column operations $\text{Add}_i^{-az,1}$ and $\text{Add}_i^{-az,2}$ to sweep out all entries below and to the right of the leading 2×2 block. After theses row-column operations, any entry below or to the right of the leading 2×2 block are

$$a - a^2 z - a(a+1)z \equiv a(1 - (2a+1)z) \equiv a(1-1) \equiv 0 \mod 2^r.$$

However, any non-diagonal entry not in the first or second row or column will be

$$\begin{aligned} a - a^2 z - a^2 z &\equiv a - 2a^2 z - az + az \mod 2^r \\ &\equiv a(1 - (2a+1)z + z) \mod 2^r \\ &\equiv az \mod 2^r \end{aligned}$$

and each diagonal entry not in the first or second row or column will be $az+1$. Let $S \in M_{k-1}(\mathbb{Z})$ be the product of all matrices S_i associated to each row-column operation. Then

$$S^{\text{tr}} T_{k,a} S \equiv \begin{pmatrix} a+1 & a \\ a & a+1 \end{pmatrix} \oplus T_{k-2,az} \mod 2^r.$$

Take note that S has determinant 1 since each S_i has determinant 1. By Lemma 2.2.9 if $a \equiv 1 \mod 4$, then there exists a matrix $S' \in M_2(\mathbb{Z})$ such that $(S')^{\text{tr}} \left(\begin{smallmatrix} a+1 & a \\ a & a+1 \end{smallmatrix}\right) S' \equiv \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ and if $a \equiv 3 \mod 4$ then there exists a matrix $S' \in M_2(\mathbb{Z})$ such that $(S')^{\text{tr}} \left(\begin{smallmatrix} a+1 & a \\ a & a+1 \end{smallmatrix}\right) S' \equiv \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Now since a is odd by assumption, $2a \equiv 2 \mod 4$. Hence, z is equivalent to $3 \mod 4$. This implies that if $a \equiv 1 \mod 4$, then $az \equiv 3 \mod 4$ and if $a \equiv 3 \mod 4$ then $az \equiv 1 \mod 4$. Thus, our inductive process yields an alternating direct sum of matrices $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ beginning with the first.

In the case when k is even, our inductive process will leave us with a 1×1 block (c). Since each 2×2 matrix has odd determinent, the 2-valuation of the c will be the same as the 2-valuation of the determinant of $T_{k,1}$. Let $\mathbf{v}_{k-1} \in (\mathbb{Z}/2^r\mathbb{Z})^{k-1}$ be the column vector with

all entries equal to 1. Since $H_{k-1} = vv^{\mathrm{tr}}$, by Sylvestor's determinant theorem $\det(T_{k,1}) = 1 + v^{\mathrm{tr}}v = k$. This implies that $v_2(c) = v_2(k)$. Then there exists an integer s such that $s^2 c \equiv \beta 2^{v_2(k)} \mod 2^r$ for some $\beta \in \{1, -1, 5, -5\}$. This completes the proof. □

Lemma 3.3.8. *Let (G, b) be a discriminant form for a 2-group G, and let n be a positive integer and a be an odd positive integer. Let q be a quadratic form such that $b_q = b$. Then*

$$\Theta(G^{2^n a-1}, T_{2^n a} \otimes q) = (-1)^{\Gamma}\sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta} \tag{3.9}$$

for particular integers β and Γ that only depend on G, n, and a (they don't depend on q).

Proof. Consider that

$$(G, q) \cong \bigoplus_{i=1}^{m}(H_i, \mu_i)$$

where $(H_i, \mu_i) = \left(\mathbb{Z}/2^{r_i}\mathbb{Z}, 2^{-r_i-1}\alpha_i x^2\right)$ or $(H_i, \mu_i) = \left((\mathbb{Z}/2^{r_i}\mathbb{Z})^2, 2^{-r_i}(\alpha_i x_1^2 + x_1x_2 + \alpha_i x_2^2)\right)$. We also know by the Fundamental Theorem of Finite Abelian Groups

$$G \cong \bigoplus_{r=1}^{\infty}(\mathbb{Z}/2^r\mathbb{Z})^{N_r}$$

Notice that for each integer r, $N_r = \sum_{i:r_i=r}\mathrm{rank}(H_i)$. Now by Lemma 3.3.7,

$$T_{2^n a} \cong \left(\bigoplus_{i=1}^{\lfloor\frac{k+1}{4}\rfloor}\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}\right) \oplus \left(\bigoplus_{j=1}^{\lfloor\frac{k-1}{4}\rfloor}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right) \oplus [\beta 2^n]$$

in $M_{2^n-1}(\mathbb{Z}/2\exp(G)\mathbb{Z})$ for $\beta \in \{1, -1, 5, -5\}$. Let

$$\Gamma = \sum_{r=1}^{\infty} N_r(r\lfloor(k+1)/4\rfloor + \max\{r-n, 0\}(\beta^2-1)/8)$$

Note that Γ and β only depend on G, n, and a. Now that we have defined Γ and β, by Lemma 2.3.3 the left hand side of equation (3.9) is equal to

$$\prod_{i=1}^{m}\Theta(H_i^{2^n a-1}, T_{2^n a} \otimes \mu_i) \tag{3.10}$$

Now for all $i \in [m]$,

$$\begin{aligned}\Theta(H_i^{2^n a-1}, T_{2^n a} \otimes \mu_i) &= \Theta\left(H_i^2, \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix} \otimes \mu_i(x)\right)^{\lfloor\frac{k+1}{4}\rfloor}\Theta\left(H_i^2, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \otimes \mu_i(x)\right)^{\lfloor\frac{k-1}{4}\rfloor}\Theta(H_i, \beta 2^n\mu_i(x))\\ &= (-1)^{\mathrm{rank}(H_i)r_i\lfloor\frac{k+1}{4}\rfloor}(1)^{\lfloor\frac{k-1}{4}\rfloor}\sqrt{|H_i[2^n]|}(-1)^{\mathrm{rank}(H_i)\max\{r_i-n,0\}(\beta^2-1)/8}\mathbf{e}(\sigma_n(b_{\mu_i})/8)^{\beta}\end{aligned}$$

And so we have

$$\begin{aligned}\prod_{i=1}^{m}\Theta(H_i^{2^n a-1},T_{2^n a}\otimes\mu_i) &= \sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}\prod_{i=1}^{m}(-1)^{\operatorname{rank}(H_i)(r_i\lfloor\frac{k+1}{4}\rfloor+\max\{r_i-n,0\}(\beta^2-1)/8)}\\ &= \sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}\prod_{r=1}^{\infty}\prod_{i\,:\,r_i=r}(-1)^{\operatorname{rank}(H_i)(r_i\lfloor\frac{k+1}{4}\rfloor+\max\{r_i-n,0\}(\beta^2-1)/8)}\\ &= \sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}\prod_{r=1}^{\infty}(-1)^{N_r(r\lfloor\frac{k+1}{4}\rfloor+\max\{r-n,0\}(\beta^2-1)/8)}\\ &= (-1)^{\Gamma}\sqrt{|G[2^n]|}\mathbf{e}\left(\frac{\sigma_n(b)}{8}\right)^{\beta}\end{aligned}$$

Thus, the lemma is proven. □

Lemma 3.3.9. *Let (G,b) and (G,b') be two discriminant forms for a 2-group G. Let (G,q) and (G,q') be the associated metric groups respectively. Then*

$$\Theta(G^{k-1},T_k\otimes q)=\Theta(G^{k-1},T_k\otimes q')$$

if k is odd or if $v_2(k)>v_2(\exp(G))$.

Proof. We know that for $n=n_1+n_2$ and $n'=n_1'+n_2'$ we have

$$(G,q)\cong(H_1,q_1)\perp\ldots\perp(H_n,q_n)\quad\text{ and }\quad(G,q')\cong(H_1',q_1')\perp\ldots\perp(H_{n'}',q_{n'}')$$

For some integers N_r we have

$$G\cong\bigoplus_r(\mathbb{Z}/2^r)^{N_r}$$

and since $\sum_{r_i=r}\operatorname{rank}(H_i)=N_r=\sum_{r_i'=r}\operatorname{rank}(H_i')$ we have

$$\sum_{i=1}^{n}r_i\operatorname{rank}(H_i)=\sum_r rN_r=\sum_{i=1}^{n'}r_i'\operatorname{rank}(H_i')$$

and thus $\sum_{i=1}^{n_1}r_i\equiv\sum_{i=1}^{n_1'}r_i'\mod 2$.

Case 1: If k is odd, Lemma 3.3.7 and Lemma 2.4.14 imply

$$\begin{aligned}\Theta(G^{k-1},T_k\otimes q) &= \prod_{i=1}^{n}\Theta(H_i^{k-1},T_k\otimes q_i)\\ &= \prod_{i=1}^{n}\Theta\left(H_i^2,\begin{pmatrix}2&1\\1&2\end{pmatrix}\otimes q_i\right)^{\lfloor\frac{k+1}{4}\rfloor}\Theta\left(H_i^2,\begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes q_i\right)^{\lfloor\frac{k-1}{4}\rfloor}\\ &= (-1)^{\lfloor\frac{k+1}{4}\rfloor\sum_{i=1}^{n_1}r_i}\end{aligned}$$

Since this expression does not depend on q, the case is proven.

Case 2: If $v_2(k) > v_2(\exp(G))$, then $\max\{r - v_2(k), 0\} = 0$ for all r such that $N_r > 0$ and $\left(\frac{\sigma_{v_2(k)}(b)}{8}\right) = 1 = \left(\frac{\sigma_{v_2(k)}(b')}{8}\right)$. Lemma 3.3.8 and Definition 2.4.11 implies

$$\begin{aligned}\Theta(G^{k-1}, T_k \otimes q) &= \prod_{i=1}^{n} \Theta(H_i^{k-1}, T_k \otimes q_i) \\ &= \prod_{i=1}^{n} \Theta\left(H_i^2, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \otimes q_i\right)^{\lfloor \frac{k+1}{4} \rfloor} \Theta\left(H_i^2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes q_i\right)^{\lfloor \frac{k-1}{4} \rfloor} \sqrt{|H_i|} \\ &= \sqrt{|G|}(-1)^{\lfloor \frac{k+1}{4} \rfloor \sum_{i=1}^{n_1} r_i}\end{aligned}$$

Since $\sum_{i=1}^{n_1} r_i \equiv \sum_{i=1}^{n_1'} r_i' \mod 2$ the expression does not depend on q. This proves the lemma. □

Theorem 3.3.10. *Let (G, b_1) and (G, b_2) be a discriminant forms. Let $\tau = \pm|G|^{-1/2}$. Let $\mathcal{C}_1 = \mathcal{TY}(G, b_1, \tau)$ and $\mathcal{C}_2 = \mathcal{TY}(G, b_2, \tau)$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are inequivalent as spherical fusion categories then there exists a positive integer k such that $\nu_{2k}(m_1) \neq \nu_{2k}(m_2)$.*

Proof. Let (G_o, b_i^o) and (G_e, b_i^e) be discriminant forms such that $|G_o|$ is odd, $|G_e|$ is a power of 2, and $(G, b_i) = (G_o, b_i^o) \perp (G_e, b_i^e)$ for $i \in \{1, 2\}$.

Let q_i, q_i^o, and q_i^e be quadratic forms such that $b_{q_i} = b_i$, $b_{q_i^o} = b_i^o$, and $b_{q_i^e} = b_i^e$ respectively for $i \in \{1, 2\}$. Theorem 3.2.4 and Lemma 3.3.2 tell us

$$\nu_{2k}(m_i) = \Theta(G^{k-1}, T_k \otimes q_i) = \Theta(G_o^{k-1}, T_k \otimes q_i^o)\Theta(G_e^{k-1}, T_k \otimes q_i^e)$$

for $i \in \{1, 2\}$.

Either $(G_o, b_1^o) \ncong (G_o, b_2^o)$, or $(G_e, b_1^e) \ncong (G_e, b_2^e)$, or both.

Case 1: If $(G_o, b_1^o) \ncong (G_o, b_2^o)$, then Lemma 3.3.6 implies there exists an integer k which is either odd or $v_2(k) > v_2(\exp(G_e))$ such that

$$\Theta(G_o^{k-1}, T_k \otimes q_1^o) \neq \Theta(G_o^{k-1}, T_k \otimes q_2^o).$$

Since k is either odd or $v_2(k) > v_2(\exp(G_e))$, Lemma 3.3.9 tells us

$$\Theta(G_e^{k-1}, T_k \otimes q_1^e) = \Theta(G_e^{k-1}, T_k \otimes q_2^e).$$

Thus $\nu_{2k}(m_1) \neq \nu_{2k}(m_2)$.

Case 2: If $(G_o, b_1^o) \cong (G_o, b_2^o)$, then by our assumption $(G_e, b_1^e) \ncong (G_e, b_2^e)$. By Theorem 2.4.12 there exists a positive integer n such that $\sigma_n(b_1^e) \neq \sigma_n(b_2^e)$. Lemma 3.3.8 tells us

$$\begin{aligned}\Theta(G_e^{\exp(G_o)2^n-1}, T_{\exp(G_o)2^n} \otimes q_1^e) &= \sqrt{|G_e[2^n]|}(-1)^\Gamma \mathbf{e}\left(\frac{\sigma_n(b_1^e)}{8}\right)^\beta \\ &\neq \sqrt{|G_e[2^n]|}(-1)^\Gamma \mathbf{e}\left(\frac{\sigma_n(b_2^e)}{8}\right)^\beta \\ &= \Theta(G_e^{\exp(G_o)2^n-1}, T_{\exp(G_o)2^n} \otimes q_2^e).\end{aligned}$$

For a positive integer Γ and $\beta \in \{1, -1, 5, -5\}$. Thus $\nu_{2(2^n)}(m_1) \neq \nu_{2(2^n)}(m_2)$. This completes the theorem. □

3.4 The State-Sum Invariant

Given a compact 3-manifold M and a spherical category $\mathcal{C}$ one can define an invariant $|M|_\mathcal{C} \in \mathbb{C}$, called the state-sum invariant, see [20]. Recently it was shown that $|M|_\mathcal{C} = \tau_{\mathcal{Z}(\mathcal{C})}(M)$ where $\mathcal{Z}(\mathcal{C})$ is the Drinfeld center of $\mathcal{C}$ and $\tau_{\mathcal{Z}(\mathcal{C})}(M)$ is the Reshetikhin-Turaev invariant. For $k \geq 1$ let

$$L_k = L_{k,1} = \{(z_1, z_2) \in \mathbb{C}^2 : |z_1|^2 + |z_2|^2 = 1\} / \left\langle (z_1, z_2) \sim e^{2\pi i/k}(z_1, z_2) \right\rangle$$

denote the lens spaces. In order to state a theorem from [20] we must first introduce some of the notation from that paper.

Definition 3.4.1. Let (G, b) be a discriminant form. Let $\varphi \in C(b)$ as defined in Definition 3.1.2. Then let

$$\gamma(\varphi) = |G|^{-1/2} |\operatorname{Rad}(b)|^{-1/2} \sum_{x \in G} \mathbf{e}(\varphi(x)) \in \mathbb{C}.$$

For any $k \geq 0$ let

$$\zeta_k(b) = |G|^{-1/2} |G[k]|^{-1/2} \sum_{\varphi \in C(b)} \gamma(\varphi)^k \in \mathbb{C}.$$

Theorem 3.4.2 ([20] Theorem 0.3)**.** *Let (G, b) be a non-degenerate discriminant form, and let $\tau = \pm|G|^{-1/2}$. Let $\mathcal{C} = \mathcal{TY}(G, b, \tau)$ be a Tambara-Yamagami category. For any odd integer*

$k \geq 1$, we have

$$|L_k|_{\mathcal{C}} = \frac{|G[k]|}{2|G|}. \tag{3.11}$$

For any even integer $k \geq 0$, we have

$$|L_k|_{\mathcal{C}} = \frac{|G[k]| + \mathrm{sgn}(\tau)^{k/2}|G|^{1/2}|G[k/2]|^{1/2}\zeta_{k/2}(b)}{2|G|}. \tag{3.12}$$

Lemma 3.4.3. *Let (G, b) be a non-degenerate discriminant form, and let $\tau = \pm|G|^{-1/2}$. Let $\mathcal{C} = \mathcal{TY}(G, b, \tau)$ be a Tambara-Yamagami category. For any integer $k \geq 1$, we have*

$$|L_k|_{\mathcal{C}} = \frac{1}{\mathrm{pdim}(\mathcal{C})} \sum_{V \in \mathrm{Irr}(C)} \nu_k(V)\,\mathrm{pdim}(V)$$

where $\mathrm{Irr}(C)$ is the set of isomorphism classes of simple objects of C.

Proof. From Theorem 3.2.4 $\sum_{g\in G} \nu_k(g) = |G[k]|$. Since $\mathrm{pdim}(g) = 1$ for all $g \in G$ and $\nu_k(m) = 0$ when k is odd, the odd case is proven. Since $\mathrm{pdim}(m) = |G|^{1/2}$, to prove the other case it is enough to show that when k is even,

$$\nu_k(m) = \mathrm{sgn}(\tau)^{k/2}|G[k/2]|^{1/2}\zeta_{k/2}(b).$$

From Equation (3.4) in the proof of Theorem 3.2.4 when k is even

$$\begin{aligned}
\nu_k(m) &= |G|^{-1/2} \sum_{\varphi\in C(b)} \left(\mathrm{sgn}(\tau)|G|^{-1/2} \sum_{x\in G} \mathbf{e}(\varphi(x)) \right)^{k/2} \\
&= |G|^{-1/2} \sum_{\varphi\in C(b)} (\mathrm{sgn}(\tau)\gamma(\varphi))^{k/2} \\
&= \mathrm{sgn}(\tau)^{k/2}|G[k/2]|^{1/2}\zeta_{k/2}(b)
\end{aligned}$$

This completes the proof. □

We denote by $\nu_n(H)$ the n-th Frobenius-Schur indicator of the regular representation of a semisimple quasi-Hopf algebra H. These numbers are interesting in the representation theory of Hopf algebras in view of their monoidal Morita invariance in the following way. Let H and L be two semisimple quasi-Hopf algebras. If $\mathrm{Rep}(H)$ and $\mathrm{Rep}(L)$ are monoidally equivalent, then $\nu_n(H) = \nu_n(L)$ for all n. (See [5]). For any pivotal fusion category $\mathcal{C}$ let $\nu_n(\mathcal{C}) =$

$\sum_{V\in\mathrm{Irr}(C)}\nu_n(V)\,\mathrm{pdim}(V)$. It is stated in [18] that by Corollary 7.8 of [14] that if $\mathcal{C}=\mathrm{Rep}(H)$ for some Hopf algebra H then

$$\nu_n(\mathcal{C})=\nu_n(H).$$

where $\nu_n(H)$ is the Frobenius-Schur indicator of the regular representation of H. Then Lemma 3.4.3 gives us the following corollary.

Corollary 3.4.4. *Let H be a semisimple quasi-Hopf algebra such that* $\mathrm{Rep}(H)$ *is a Tambara-Yamagami category. Then*

$$\dim(H)|L_n|_{\mathrm{Rep}(H)}=\nu_n(H).$$

where L_n is the lens space as defined above.

[20] proved that if $\mathcal{C}=\mathcal{TY}(G,b,\tau)$ and $\mathcal{C}'=\mathcal{TY}(G',b',\tau')$ such that $|M|_{\mathcal{C}}=|M|_{\mathcal{C}'}$ for all 3-manifolds M and $|G|$ is odd, then $\mathcal{C}$ and $\mathcal{C}'$ are monoidally equivalent. They conjectured that this statement is true for all Tambara-Yamagami categories. We are able to make a slightly stronger statement, and also show that the lens spaces L_k are not enough to prove the conjecture.

Theorem 3.4.5. *Let $\mathcal{C}=\mathcal{TY}(G,b,\tau)$ and $\mathcal{C}'=\mathcal{TY}(G',b',\tau')$ such that $|M|_{\mathcal{C}}=|M|_{\mathcal{C}'}$ for all 3-manifolds M. If $|G|$ is not a power of 2, then $\mathcal{C}$ and $\mathcal{C}'$ are monoidally equivalent.*

Proof. Let G_e and G'_e be the 2-sylow subgroups of G and G' respectively. Let G_o and G'_o be the direct sum of p-sylow subgroups for all odd primes p for G and G' respectively. We see that $|G|=\frac{1}{2|L_1|_{\mathcal{C}}}=|G'|$. Also, the fact that $G[k]=2|G||L_k|_{\mathcal{C}}=G'[k]$ for all odd k implies $G_o\cong G'_o$. Thus $|G_e|=|G'_e|$. By Theorem 3.3.10 it is enough to show that $G\cong G'$. We will prove this by contradiction.

Assume that $G_e\ncong G'_e$. Since $G_e[0]=1=G'_e[0]$, we may pick the smallest $n\geq 0$ such that, without loss of generality, $|G[2^{n+1}]|>|G'[2^{n+1}]|$ and $|G[2^m]|=|G[2^m]|$ for all $m\leq n$.

Let $a=|G_o|=|G'_o|$. Let $m\geq 0$. Then $G[a2^m]=G_o\oplus G[2^m]$. By Theorem 3.2.5, we can write $\nu_{a2^{m+1}}(m_{\mathcal{C}})=|G[a2^m]|^{1/2}\xi_m$ where $\xi_m\in\mu_8\cup\{0\}$. Define ξ'_m similarly for $\mathcal{C}'$. We have

$$2|G||L_{a2^{m+1}}|_{\mathcal{C}}=|G[a2^{m+1}]|+|G|^{1/2}\nu_{a2^{m+1}}(m_{\mathcal{C}})=|G_o|\left(|G[2^{m+1}]|+|G_e|^{1/2}|G[2^m]|^{1/2}\xi_m\right).$$

So $|L_{a2^{m+1}}|_{\mathcal{C}} = |L_{a2^{m+1}}|_{\mathcal{C}'}$ implies

$$|G[2^{m+1}]| + |G_e|^{1/2}|G[2^m]|^{1/2}\xi_m = |G'[2^{m+1}]| + |G'_e|^{1/2}|G'[2^m]|^{1/2}\xi'_m. \tag{3.13}$$

Since $|G[2^{n+1}]| \neq |G'[2^{n+1}]|$ the equation above implies we cannot have $\xi_n = \xi'_n = 0$. Without loss of generality, assume $\xi_n \neq 0$. Since $|G_e| = |G'_e|$ and $|G[2^n]| = |G'[2^n]|$ we may rearrage equation (3.13) to get

$$|G[2^{n+1}]| - |G'[2^{n+1}]| = |G_e|^{1/2}|G[2^n]|\xi_n((\xi'_n/\xi_n) - 1). \tag{3.14}$$

Each side of equation (3.14) belong to $\mathbb{Z}[e^{2\pi i/8}]$. Consider the absolute norm of each side. Since $\xi_n \in \mu_8$, one verifies that the absolute norm of $(\xi_n - 1)$ is a power of 2 or zero. For example if ξ_n is a primitive 8-th root of unity, then

$$N_{\mathbb{Q}}^{\mathbb{Q}[\xi_n]}(\xi_n - 1) = \left(\mathbf{e}\left(\frac{1}{8}\right) - 1\right)\left(\mathbf{e}\left(\frac{3}{8}\right) - 1\right)\left(\mathbf{e}\left(\frac{5}{8}\right) - 1\right)\left(\mathbf{e}\left(\frac{7}{8}\right) - 1\right) = 2.$$

So the norm of both sides of equation (3.14) is a power of 2. However, the only way this holds for the left hand side is if $|G[2^{n+1}]| = 2|G'[2^{n+1}]|$.

Now write $\nu_{2^{n+1}}(m_{\mathcal{C}}) = |G[2^n]|^{1/2}\lambda_n$ and $\nu_{2^{n+1}}(m_{\mathcal{C}'}) = |G[2^n]|^{1/2}\lambda'_n$ for some $\lambda_n, \lambda'_n \in \mu_8 \cup \{0\}$ (Notice we made use of the fact that $|G[2^n]| = |G'[2^n]|$). Now the equality $|L_{2^{n+1}}|_{\mathcal{C}} = |L_{2^{n+1}}|_{\mathcal{C}'}$ yields

$$|G'[2^{n+1}]| = |G[2^{n+1}]| - |G'[2^{n+1}]| = |G|^{1/2}|G[2^n]|^{1/2}(\lambda_n - \lambda'_n).$$

Now the left hand side is a power of 2, so norm of the right-hand side must also be a power of 2. Since $N(\lambda_n - \lambda'_n)$ is a power of 2, this forces $|G|$ to be a power of 2, which contradicts our hypothesis. □

It is not possible to prove the conjecture by Turaev and Vainerman with only the state-sums of the lens spaces by the following example.

Example 3.4.6. Recall that A_{2^n} denotes the metric group $((\mathbb{Z}/2^n\mathbb{Z}), x^2/2^{n+1})$ and the corresponding discriminant form. Let $(G_1, b_1) = (A_2)^4 \perp A_4$ and $(G_2, b_2) = (A_2)^2 \perp (A_4)^2$. Let $\mathcal{C}_1 = \mathcal{TY}(G_1, b_1, -\frac{1}{8})$ and $\mathcal{C}_2 = \mathcal{TY}(G_2, b_2, \frac{1}{8})$. Then we claim that $|L_n|_{\mathcal{C}_1} = |L_n|_{\mathcal{C}_2}$ for all positive integers n.

Proof. Let q_i be a quadratic form such that $b_{q_i} = b_i$ for $i \in \{1, 2\}$. We will break the proof into cases according to possible 2-valuations of n. The trivial case is that $|L_n|_{\mathcal{C}_1} = \frac{1}{128} = |L_n|_{\mathcal{C}_2}$ if n is odd. By Lemma 3.4.3, Theorem 3.2.4, and Lemma 3.3.2 to prove that $|L_{2k}|_{\mathcal{C}_1} = |L_{2k}|_{\mathcal{C}_2}$ it is enough to show that

$$G_1[2k] + (-1)^k\sqrt{|G_1|}\Theta(G_1^{k-1}, T_k \otimes q_1) = G_2[2k] + \sqrt{|G_2|}\Theta(G_2^{k-1}, T_k \otimes q_2).$$

Since Θ is multiplicative,

$$\Theta(G_1^{k-1}, T_k \otimes q_1) = \Theta\left((\mathbb{Z}/2\mathbb{Z})^{k-1}, T_k \otimes (x^2/4)\right)^4 \Theta\left((\mathbb{Z}/4\mathbb{Z})^{k-1}, T_k \otimes (x^2/8)\right)$$
$$\Theta(G_2^{k-1}, T_k \otimes q_2) = \Theta\left((\mathbb{Z}/2\mathbb{Z})^{k-1}, T_k \otimes (x^2/4)\right)^2 \Theta\left((zz/4\mathbb{Z})^{k-1}, T_k \otimes (x^2/8)\right)^2.$$

Case 1: Suppose k is odd. By Lemma 3.3.7 and Lemma 2.4.14

$$\Theta((\mathbb{Z}/2^r\mathbb{Z})^{k-1}, T_k \otimes (x^2/2^{r+1})) = (-1)^{r\lfloor (k+1)/4 \rfloor}.$$

Thus $\Theta(G_1^{k-1}, T_k \otimes q_1) = 1 = \Theta(G_2^{k-1}, T_k \otimes q_2)$. Since $\sqrt{|G_1|} = 8 = \sqrt{|G_2|}$ and $|G_1[2k]| = 32$ and $|G_2[2k]| = 16$, we get $|L_{2k}|_{\mathcal{C}_1} = |L_{2k}|_{\mathcal{C}_2}$ in this case.

Case 2: Suppose $v_2(k) = 1$ or 2. Let $i = 1$ or 2. Since (G_i, b_i) has an irreducible component of type A_2 and an irreducible component of type A_4, from Remark 3.2.7, we have $\Theta(G_i^{k-1}, T_k \otimes q_i) = 0$. Since $|G_i[2k]| = 64$, we get $|L_{2k}|_{\mathcal{C}_1} = |L_{2k}|_{\mathcal{C}_2}$ in this case.

Case 3: Finally suppose $v_2(k) \geq 3$. Let $i \in \{1, 2\}$. This case is similar to the second part of the proof of Lemma 3.3.9. Since the group $(\tilde{G}_i)_2^{v_2(k)}$ defined in Definition 2.4.11 is zero, $\mathbf{e}(\sigma_{v_2(k)}(b_i)/8) = 1$. From Lemma 3.3.8 we get

$$\Theta(G_i^{k-1}, T_k \otimes q_i) = (-1)^{\Gamma_i}|G[2^{v_2(k)}|^{1/2}(\mathbf{e}(\sigma_{v_2(k)}(b_i)/8))^{\beta_i} = 8.$$

Since $|G_i[2k]| = 64$ and $(-1)^k = 1$, we get $|L_{2k}|_{\mathcal{C}_1} = |L_{2k}|_{\mathcal{C}_2}$ in this case too. □

BIBLIOGRAPHY

[1] Bakalov, B. and Kirillov, Jr., A. (2001). *Lectures on tensor categories and modular functors*, volume 21 of *University Lecture Series*. American Mathematical Society, Providence, RI.

[2] Barrett, J. W. and Westbury, B. W. (1999). Spherical categories. *Adv. Math.*, 143(2):357–375.

[3] Etingof, P., Nikshych, D., and Ostrik, V. (2005). On fusion categories. *Ann. of Math. (2)*, 162(2):581–642.

[4] Iwaniec, H. and Kowalski, E. (2004). *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI.

[5] Kashina, Y., Montgomery, S., and Ng, S.-H. (2012). On the trace of the antipode and higher indicators. *Israel J. Math.*, 188:57–89.

[6] Kassel, C. (1995). *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[7] Kawauchi, A. and Kojima, S. (1980). Algebraic classification of linking pairings on 3-manifolds. *Math. Ann.*, 253(1):29–42.

[8] Linchenko, V. and Montgomery, S. (2000). A Frobenius-Schur theorem for Hopf algebras. *Algebr. Represent. Theory*, 3(4):347–355. Special issue dedicated to Klaus Roggenkamp on the occasion of his 60th birthday.

[9] Mason, G. and Ng, S.-H. (2005). Central invariants and Frobenius-Schur indicators for semisimple quasi-Hopf algebras. *Adv. Math.*, 190(1):161–195.

[10] Milnor, J. and Husemoller, D. (1973). *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[11] Miranda, R. (1984). Nondegenerate symmetric bilinear forms on finite abelian 2-groups. *Trans. Amer. Math. Soc.*, 284(2):535–542.

[12] Müger, M. (2003). From subfactors to categories and topology. II. The quantum double of tensor categories and subfactors. *J. Pure Appl. Algebra*, 180(1-2):159–219.

[13] Ng, S.-H. and Schauenburg, P. (2007a). Frobenius-Schur indicators and exponents of spherical categories. *Adv. Math.*, 211(1):34–71.

[14] Ng, S.-H. and Schauenburg, P. (2007b). Higher Frobenius-Schur indicators for pivotal categories. In *Hopf algebras and generalizations*, volume 441 of *Contemp. Math.*, pages 63–90. Amer. Math. Soc., Providence, RI.

[15] Nikulin, V. V. (1979). Integer symmetric bilinear forms and some of their geometric applications. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(1):111–177, 238.

[16] Schauenburg, P. (2001). Turning monoidal categories into strict ones. *New York J. Math.*, 7:257–265 (electronic).

[17] Shimizu, K. (2011). Frobenius-Schur indicators in Tambara-Yamagami categories. *J. Algebra*, 332:543–564.

[18] Shimizu, K. (2012). Some computations of Frobenius-Schur indicators of the regular representations of Hopf algebras. *Algebr. Represent. Theory*, 15(2):325–357.

[19] Tambara, D. and Yamagami, S. (1998). Tensor categories with fusion rules of self-duality for finite abelian groups. *J. Algebra*, 209(2):692–707.

[20] Turaev, V. and Vainerman, L. (2012). The Tambara-Yamagami categories and 3-manifold invariants. *Enseign. Math. (2)*, 58(1-2):131–146.

[21] Wall, C. T. C. (1963). Quadratic forms on finite groups, and related topics. *Topology*, 2:281–298.